EGI-Engage

EGI federation operations roadmap

D5.4

Date	29 August 2017
Activity	WP5
Lead Partner	EGI Foundation
Document Status	FINAL
Document Link	https://documents.egi.eu/document/3039

Abstract

This deliverable describes the current status of the EGI Operations, in terms of operations coordination activities at federation and national level, and the status of the resource infrastructure. The deliverable also describes the main areas of evolution that will have to be addressed in the coming months, after the end of the project, to keep the EGI operations effective and efficient, and be able to support the evolving service portfolio of the e-Infrastructure.

The EGI-Engage project is co-funded by the European Union (EU) Horizon 2020 program under Grant number 654142 http://go.egi.eu/eng

COPYRIGHT NOTICE

DELIVERY SLIP

	Name	***Partner/Activity***	***Date***
From:	Peter Solagna	EGI Foundation/WP5	18/08/2017
Moderated by:	Małgorzata Krakowian	EGI Foundation/WP1	
Reviewed by	Małgorzata Krakowian Matthew Viljoen	EGI Foundation/WP1 EGI Foundation/WP4	
Approved by:	AMB and PMB		29/08/2017

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author/Partner***
v.1	18/08/2017	First version of deliverable	Peter Solagna/EGI Foundation
FINAL	29/08/2017	Final version after external review	Peter Solagna/EGI Foundation

TERMINOLOGY

A complete project glossary and acronyms are provided at the following pages:

- https://wiki.egi.eu/wiki/Glossary
- https://wiki.egi.eu/wiki/Acronyms

Contents

Executive summary

The EGI production infrastructure is evolving and expanding in terms of capacity and services provided also thanks to the piloting activities of EGI-Engage.

Although the number of resource centres remains constant, the federation now has extensive coverage, both in Europe and beyond. The capacity of both computing and storage resource is steadily increasing. In details the overall usage of HTC computing resources and storage is increasing, Cloud computing usage decreased in 2016, compared to 2015, but has increased in the first part of 2017.

High energy physics remains the main community for EGI with increasing usage of HTC and storage, their relative usage of resources, compared to other communities, is increasing as well. New communities are requesting federated cloud services more than HTC.

Operations is not a static activity, it must expand and evolve together with the services offered by EGI to the users. The operations infrastructure will have to consolidate in the coming months the work of integration of new technologies carried out during the EGI-Engage project, for example EGI DataHub and applications on demand. In summary the roadmap of the Operations processes evolution will focus on ensuring that:

- New ways to access the services are properly evaluated from a operational point of view
- New technologies are following the software validation and release in production processes
- Service provisioning through SLA will improve, particularly in terms of integration with the other operations processes. For the benefit of both for the service providers and the customers
- The members of the federation will be up-to-date with the changes in the service portfolio and proper communication channels will be in place to exchange experiences and know-how on the new services
- Security controls and policies will be applicable, and applied, to the whole EGI service portfolio, and compatible with the data protection regulations

The overall goal is to ensure that new services and technologies will not degrade the reliability and security of the EGI production infrastructure, and also that the service provisioning will be sustainable with the available effort at national and EIRO level.

1. Introduction

The EGI Infrastructure is a highly distributed e-Infrastructure, federating resource centres in Europe and beyond, and serving thousands of users worldwide.

Maintaining the production infrastructure of EGI efficient and effective requires: a significant effort (distributed among resource centres, operations centres, and central coordination), and an advanced set of operations procedures, policies, and technical tools.

EGI Operations coordinate the provisioning of the production IT services in the EGI catalogue[1] and internal service catalogue[2].

The EGI-Engage project supports the central operations coordination activities, and the evolution of many operational processes including, but not limited to, security coordination, and SLA management. The project also evolved many EGI services, for example in the context of the federated cloud or AAI, and prototyped new services that soon will be in production, for example the DataHub. New services and ways to access resources require to be integrated with the operational federations of EGI and, while the project supported these integration activities, these improvements will have to be consolidated in the next months.

This document focuses on the operations coordination activities, presenting the current status of the federation and what are the open challenges, and what in which direction should operations evolve to tackle these challenges in the coming months.

A summary overview of the EGI Operations is described in section 2, with the status of the resource infrastructure, cloud and HTC, and how the resources are used by the EGI users.

The status of operations coordination activities is described in section 3, at different levels: national/EIRO operations, federation-level operations, and core activities. One input for the content of the section is a survey that has been run among the NGIs during July 2017, about the current status and the future of the EGI operations.

Finally, sections 4 and 5 describe two areas that have been re-designed and evolve during the project: technology provisioning and service level management with customers.

[1] https://www.egi.eu/services/
[2] https://www.egi.eu/internal-services/

2. Status of the resource infrastructure

In July 2017 the EGI infrastructure comprises resources provided across **47 countries**. These resources are hosted, managed, and operated by the Resource Centres (RCs).

The Resource Centres (RC) are federated in EGI through the affiliation to a NGIs (National Grid Initiative), organisations set up to manage the resources provided in their countries by the RCs to the 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 is supported by an Operations Centre, defined as a centre offering operations services on behalf of the NGI (or Resource infrastructure Provider (RP), more generally), 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 24 national Operations Centres and 7 federated Operations Centres supporting multiple NGIs. 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 project. In contrast, integrated federated centres in Asia Pacific and Latin America encompass a large number of countries, as in those regions Resource Centres are sparse and their number does not justify the overhead for the creation of a national operations centre, but suggests that an international collaboration is in place. The creation of new NGIs in those regions will depend on their expansion plans and on national policies.

The total number of certified RCs in July 2017 amounts to 265. In February 2016 the certified RCs were 312: most of the sites suspended or closed since then were medium/small size RCs that didn't have enough resources, either in terms of manpower or funding, for guaranteeing a sufficient level of service quality. Even if the number of production RCs is decreased, the capacity of the EGI infrastructure is grown, as we are showing in the next paragraphs.

Each RC has to agree on Operations Level Agreement (OLA) to be part of the EGI production infrastructure,[3] an agreement between RPs and RCs for defining the provision and support of the provided services. In the document it is described the minimum set of Functional Capabilities (for example Cloud Computing, File Transfer and Storage Management) that a RC has to provide, plus operational requirements as the minimum quality of service provisioning targets. The next sections show data about the Functional Capabilities operated by the EGI resource centres.

The policy framework that supports the EGI federation can also underpin additional policy requirements, for example provided by collaborating infrastructures or specific regulations.

[3] https://documents.egi.eu/document/31

2.1 High throughput computing resources

The HTC Compute allows users to run big numbers of loosely coupled computational tasks on distributed resources, accessible via a standard interface and supporting authorization based on virtual organisation membership. The platforms supported in EGI are: ARC-CE, CREAM, UNICORE and GLOBUS. This diversity allows EGI to support different use case by exploiting the different features provided by the software available. Since the UNICORE and GLOBUS resources do not support publishing information in the information system, for them we can provide only the number of the certified instances registered in the service registry GOC-DB, as shown in the Figure 1: Number of certified CE per type: almost the 75% of the certified computing elements in EGI runs the CREAM platform.

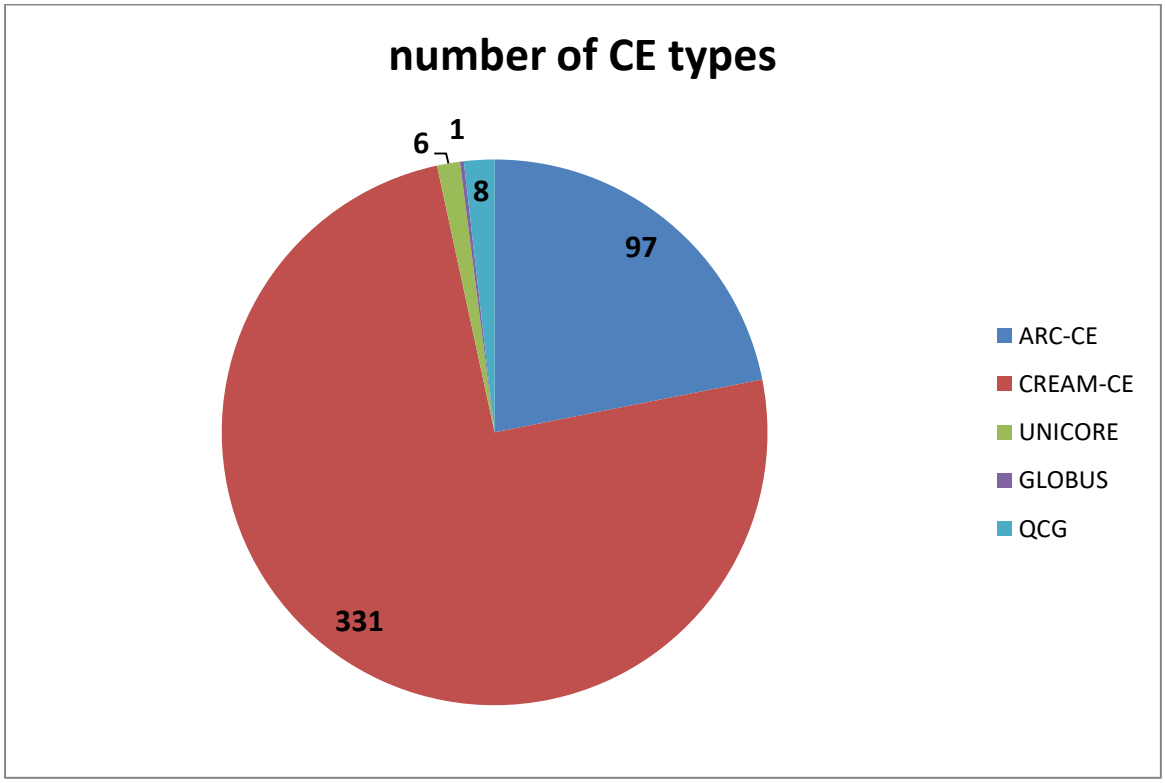


Figure 1: Number of certified CE per type

Figure 2 shows the distribution of the CE types across the NGIs.

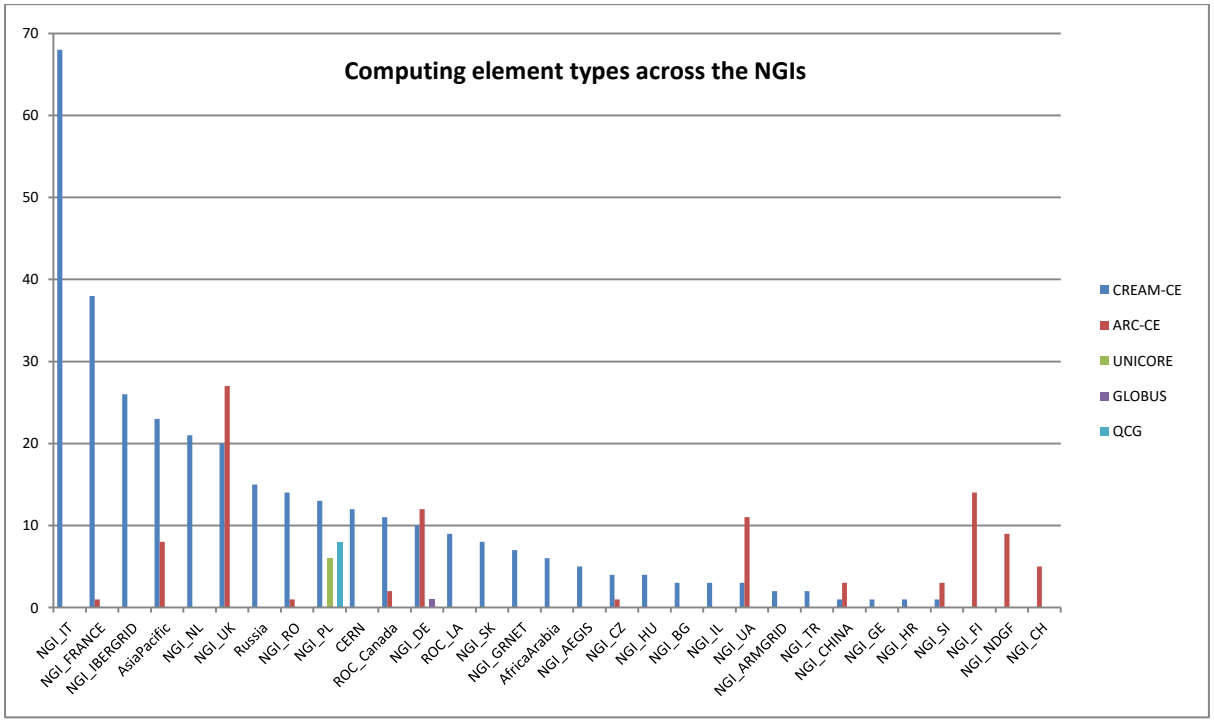


Figure 2: Computing elements distribution across the infrastructure.

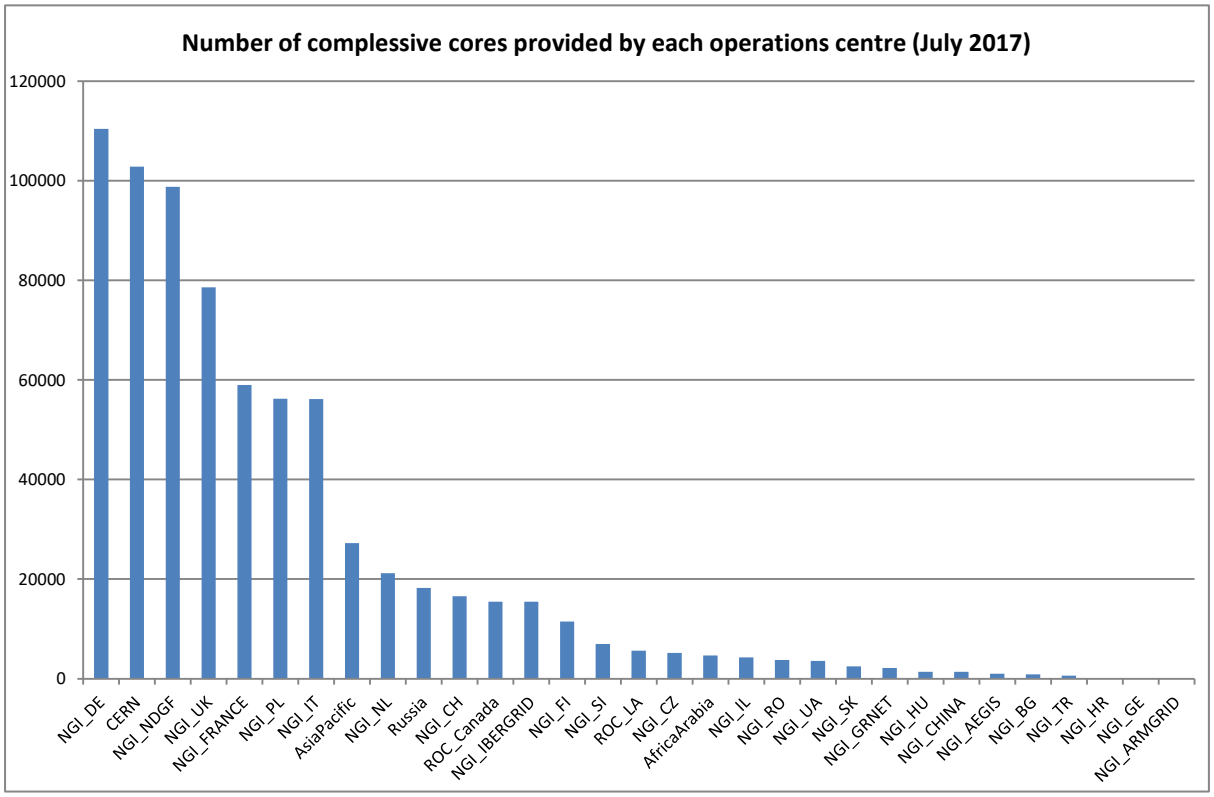
The noticeable change in the distribution of the CE technologies during the EGI-Engage project has been an increase of ARC-CE components replacing, or being installed in parallel to, CREAM-CE instances. The total amount of cores provided by the HTC Compute capability in July 2017 is more than 731800; in the table it is reported the same value collected over the past years.

Table 1: Number of cores and relative increase over the past years (July 2017).

Year	Logical cores	Increase
2014-12	527248	+21.5%
2016-02	599671	+13,74%
2016-12	681223	+13,60%
2017-07	731824	+7,43%

This metric is taken from the information system, where the RCs publish the amount of resources available to the EGI users. RCs publish in the information system the amount of resources

available through the interfaces registered in GOCDB, which may be only a subset of the total resources deployed at the RC. The size of the infrastructure is growing, as shown also in Figure 3; the contribution of each NGI to the infrastructure HTC capacity is given in



.

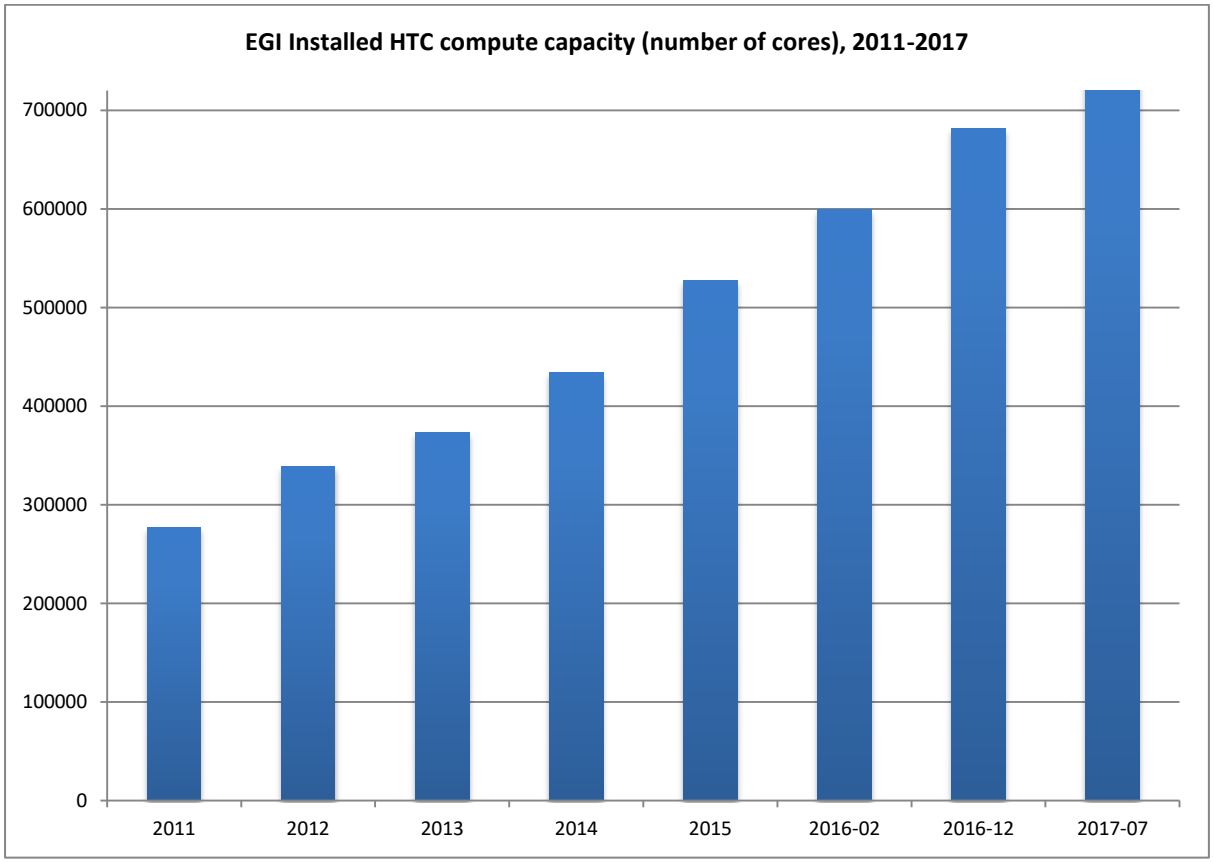


Figure 3: Number of cores over the years.

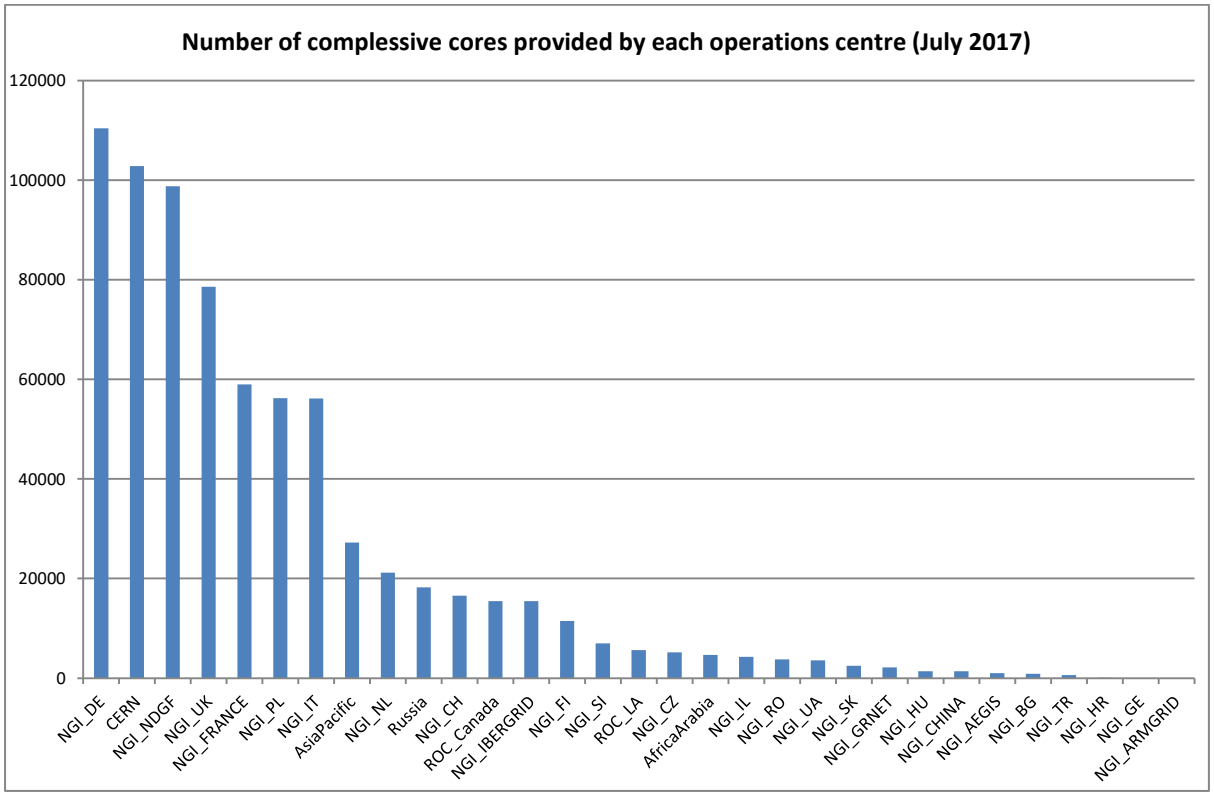


Figure 4: HTC compute capacity provided by each NGI

Compared to a similar distribution analysis done in 2015[4] the separation between operation centres with the bigger capacity and the other operations centres has increased. The EGI infrastructure provides also compute resources for parallel jobs. The numbers of resource centres that support parallel computing via MPI jobs are 41 as results in July 2017, or rather 57 computing elements in total (Figure 5). In February 2016 there were 54 RCs (67 CEs) supporting parallel jobs: even if the number of CE is decreased, the MPI computing capacity is concentrated on a fewer larger Resource Centres, and the overall capacity offered considerably increased.

[4] https://documents.egi.eu/secure/RetrieveFile?docid=2670&version=14&filename=EGI-Engage%20D5.1%20FINAL.pdf

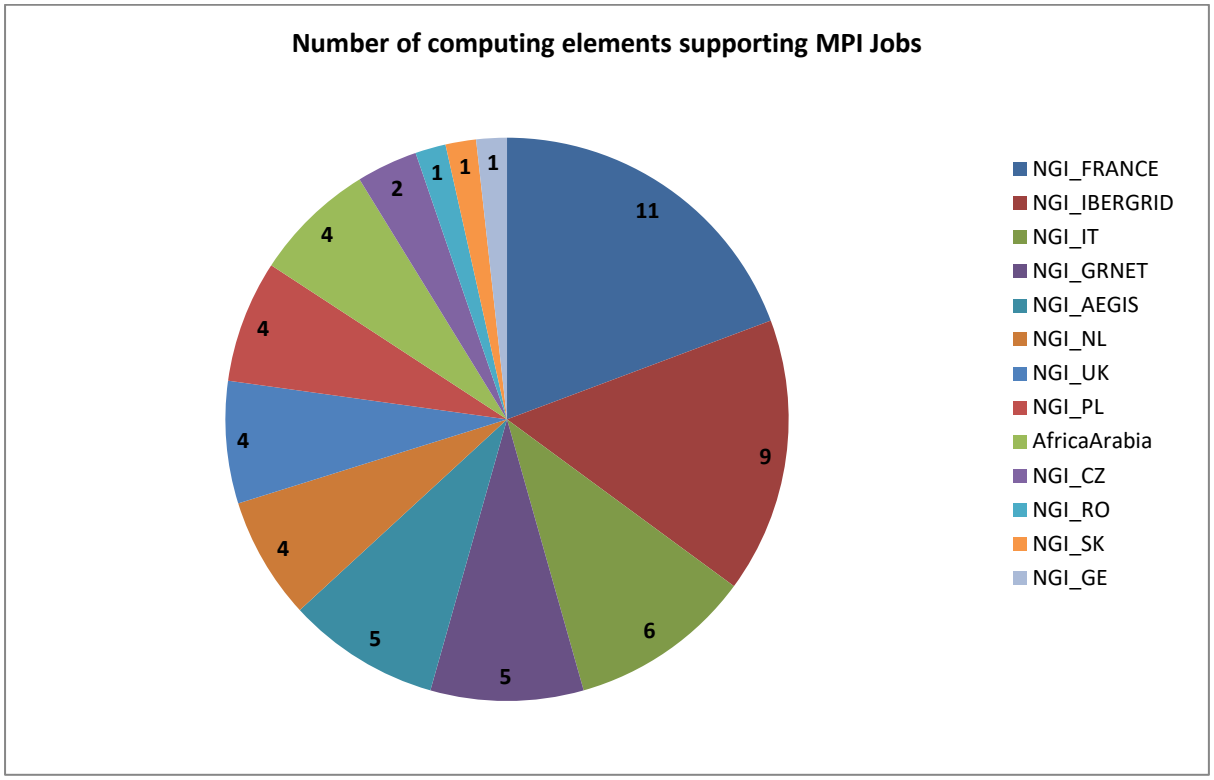


Figure 5: Number of CE supporting parallel jobs

The number of clusters supporting MPI computing tasks has increased, compared to the same analysis performed in 2015, but within a 10% difference, also the distribution across operations centers is similar.

Historically the gLite WMS service has been used as the main workload management tool for the jobs submission to the computing resources, it enables users to manage thousands of computing tasks submitted to multiple Resource Centres. gLite WMSs has been in best effort support since more than one year and in agreement with the developers it will be decommissioned by the end of 2017.

DIRAC[5] has been chosen as the EGI-supported alternative to gLite WMS. DIRAC is a tool that comprises many of the features already provided by the WMS, adding new ones.

Many VOs are already using DIRAC, but there are still communities using the gLite WMS service. After collecting some statistics about the WMS usage, EGI Operations contacted the few VOs that were mostly using this service, informing them about the decommission plans. In case there are several, or many, VO who are interested in using DIRAC as alternative to the WMS, EGI Operations will agree with them a plan for a smooth transition to DIRAC.

[5] http://diracgrid.org/

EGI provides a DIRAC instance[6] for the VOs who cannot operate a workload management system, and some new VOs have already started the process for testing before moving completely to it.

DIRAC of course is not mandatory, but is the solution suggested by EGI, and users can use any other workload management system, as long as it fits their purposes and it fulfills the EGI policies.

2.1.1 HTC resources usage

The information about the resources usage are gathered and stored centrally, accessible through the accounting portal[7].

In the first half of 2017 it was consumed 15.38 Billion HEP-SPEC 06[8] Hours, as shown in Table 2 with a relative increment of 15.52% compared with the second half of 2016 (the increment in the 2016 compared to 2015 was 22,2%), so this growth trend is expected to be confirmed at the end of the year. An increase in the resources usage was registered also for the total number of jobs executed on the infrastructure: 324.4 Millions in the first half of 2017, which corresponds to an average 1.79 Million job/day. In 2016 the average jobs/day was 1.71, instead in 2015 it was 1.59.

Table 2 HTC Compute resources usage in the last years.

	2015	2016	2017 (01-06)
Total normalized CPU time consumed (Billion HEP-SPEC 06 hours)	20.43	24.96	15.38
Total number of jobs (Million)	578.8	624.5	324.4
Average number of jobs per day (Million)	1.59	1.71	1.79

The increase of the normalized CPU time registered in the last years higher than the increased number of jobs (7.9% from 2015 to 2016, and 7.34% from 2016 to 2017) may be explained by the submission of multi-core jobs that consume more resources than the single core ones. Since 2015 the number of multi core/parallel jobs has enormously increased, showing the results of the effort of adapting scientific applications to the modern CPU architectures.

It is reported in Figure 6 and in Figure 7 the monthly trends about the HEP-SPEC06 hour usage and the number of jobs since 2015 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 consumption has increased constantly.

[6] http://dirac.egi.eu/DIRAC/
[7] https://accounting.egi.eu/
[8] http://w3.hepix.org/benchmarks/doku.php?id=homepage

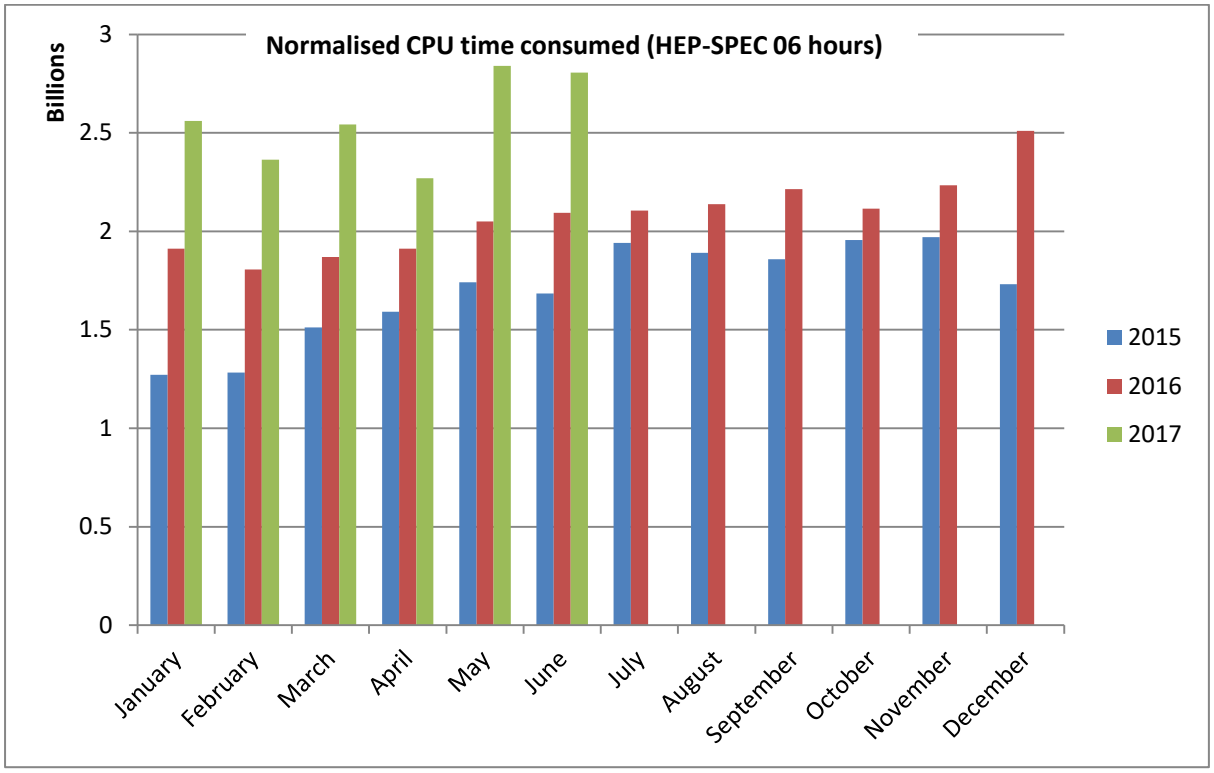


Figure 6: HEP-SPEC 06 Hours monthly usage since 2015

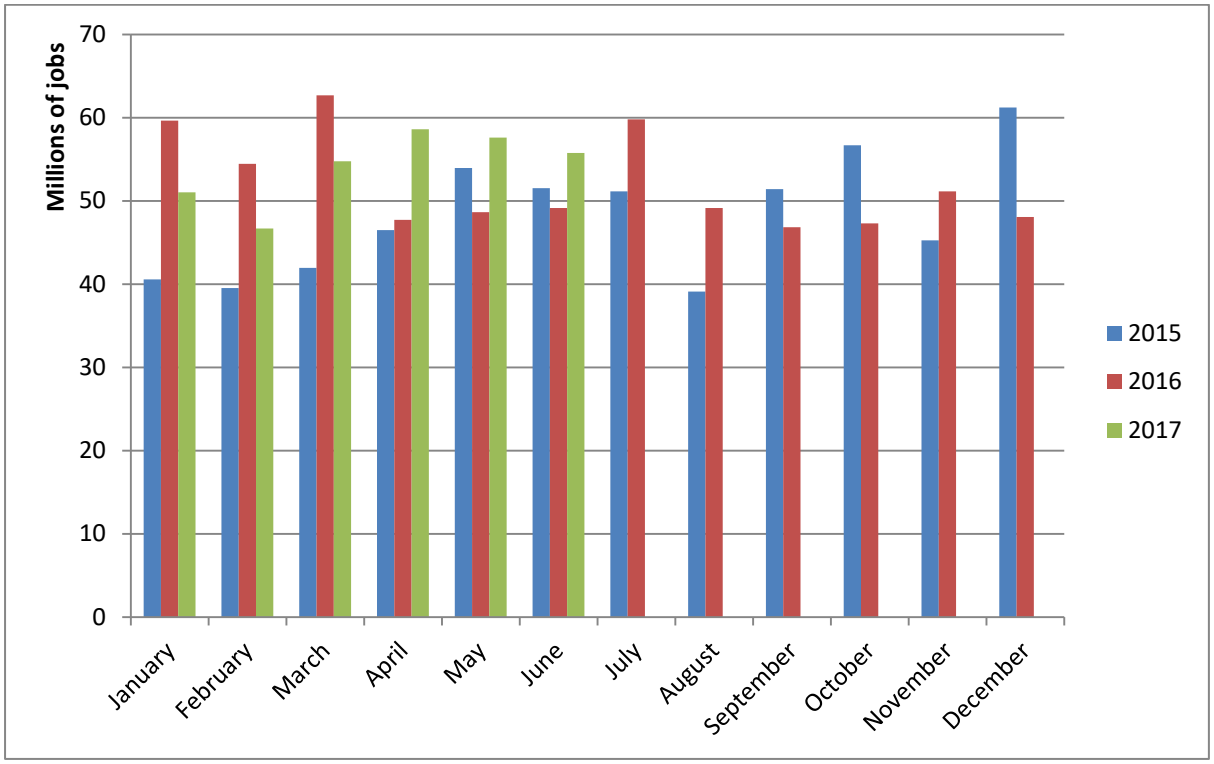


Figure 7: Number of jobs per month since 2015

The plots in Figure 8 show the total number of jobs per VO and per Operations Centre respectively, in the period between July 2016 and June 2017.

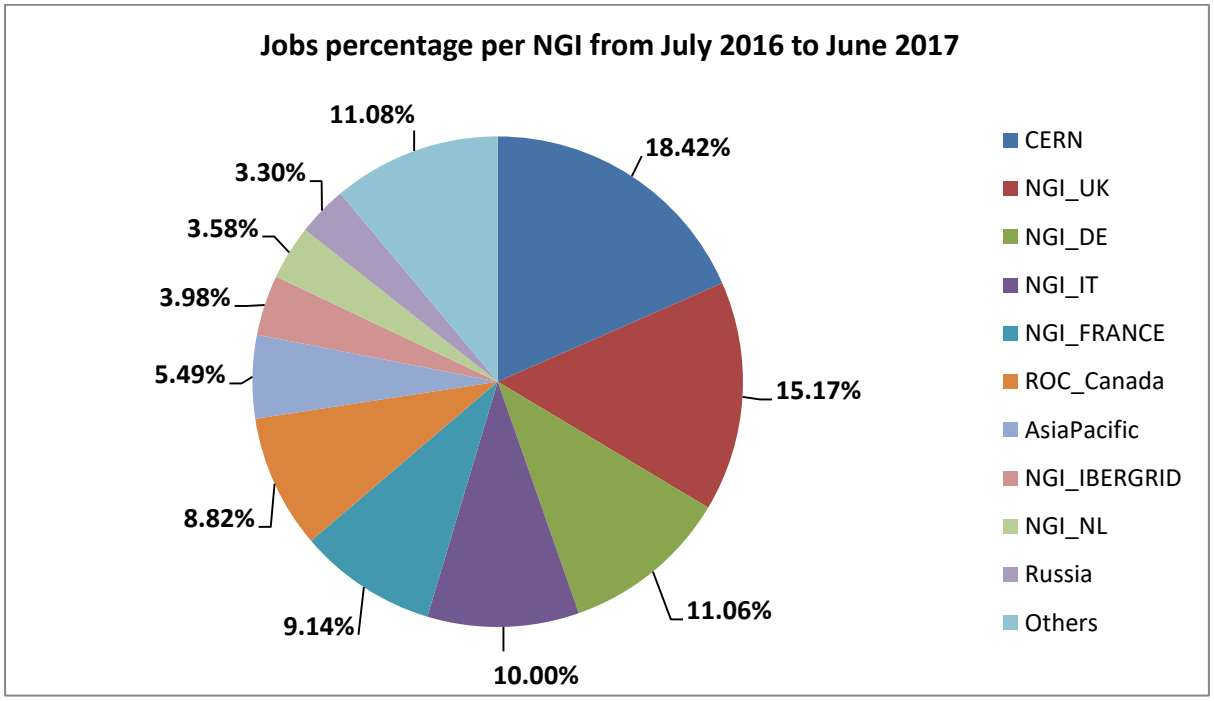


Figure 8: Total number of jobs per NGI from July 2016 to June 2017

The usage expressed in HEP-SPEC 06 Hours of CPU time across the various EGI resource providers of EGI is plotted in Figure 9. The diagram also shows the distribution between the four LHC VOs ATLAS, CMS, ALICE and LHCb (red bars) and the other VOs (blue bars).

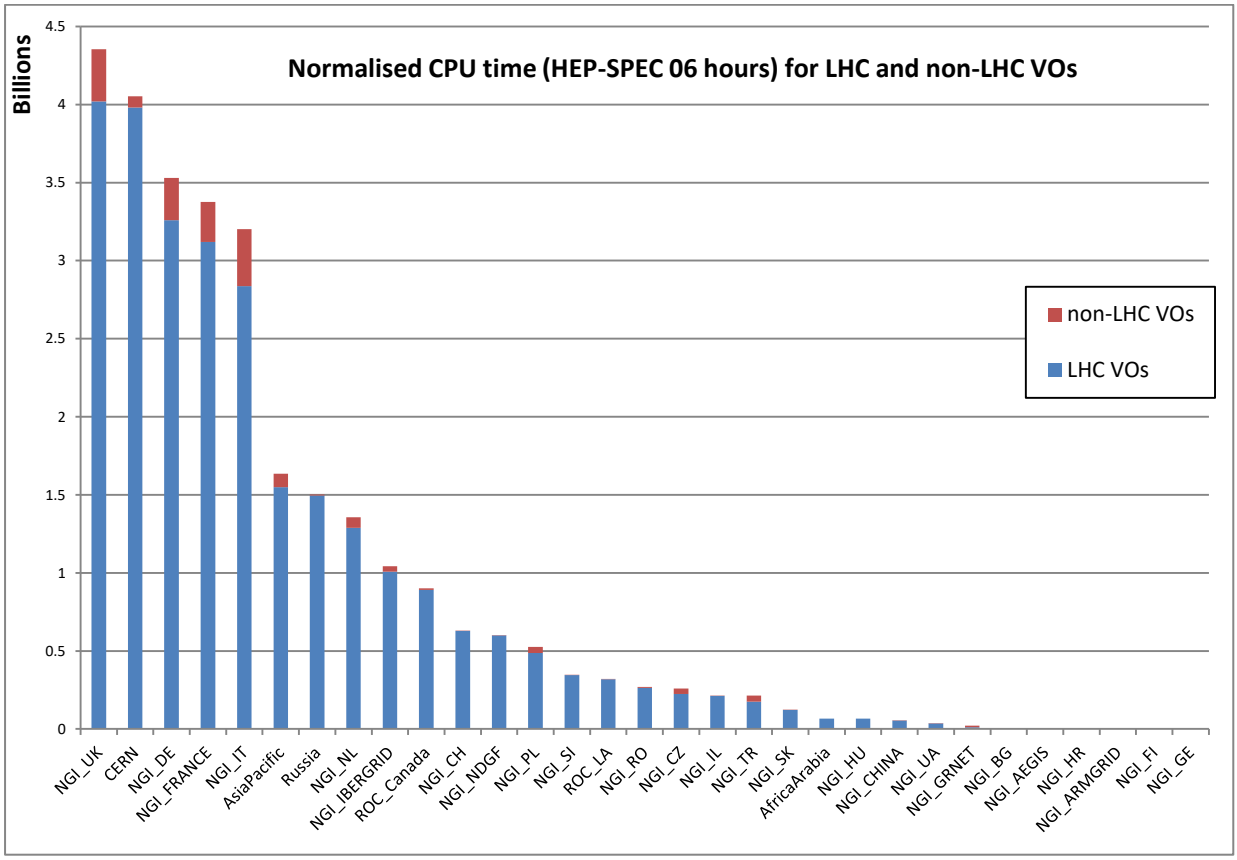


Figure 9: HEP-SPEC 06 hours consumed by LHC and non-LHC VOs from July 2016 to July 2017

As shown by the graphs above the resources are mainly consumed by the High Energy Physics (HEP) VOs, even though the level of multidisciplinary support varies considerably across the infrastructures. The most used infrastructures in absolute by all scientific disciplines (in decreasing order) are: NGI_UK, CERN, NGI_DE, NGI_FRANCE and NGI_IT, being the largest NGIs in terms of compute capacity. Focusing on the non-HEP VOs (Figure 10), we can see how the resources usage by the rest of user communities is distributed across the EGI infrastructure. Again the most used infrastructures by the non-LHC VOs are the largest ones: NGI_IT registered the largest absolute amount of usage with almost 365 million HEP-SPEC06 hours, followed by NGI_UK, NGI_DE, NGI_FRANCE.

The resources usage ratio between HEP and non-HEP VOs is shown in Figure 11 and Figure 12: the trend says that the percentage usage by LHC VOs is increasing compared to the other VOs, due to the significantly bigger increase in resource usage by the LHC VOs. But considering the current accounting data in 2017, it is reasonable to expect that at the end of this year the relative usage by non-HEP communities will be slightly higher than what recorded in 2016.

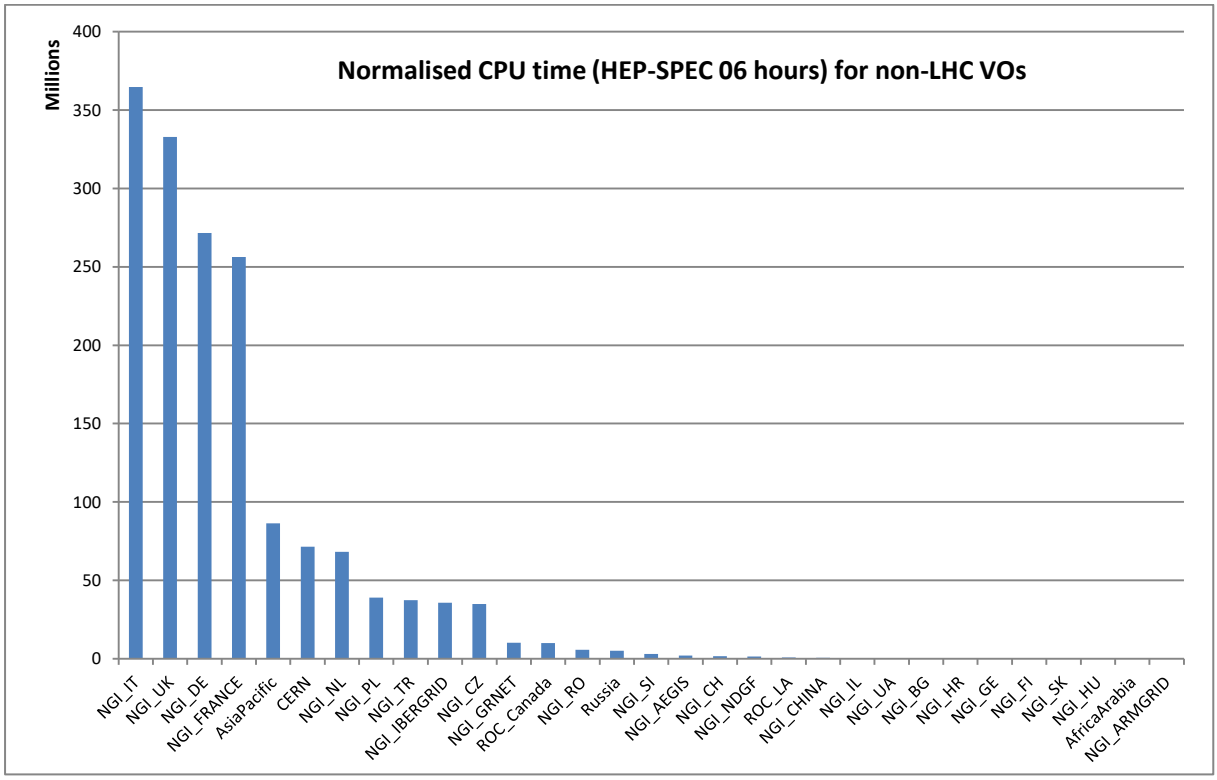


Figure 10: Normalised CPU time consumed by non-LHC VOs across the NGIs from July 2016 to June 2017

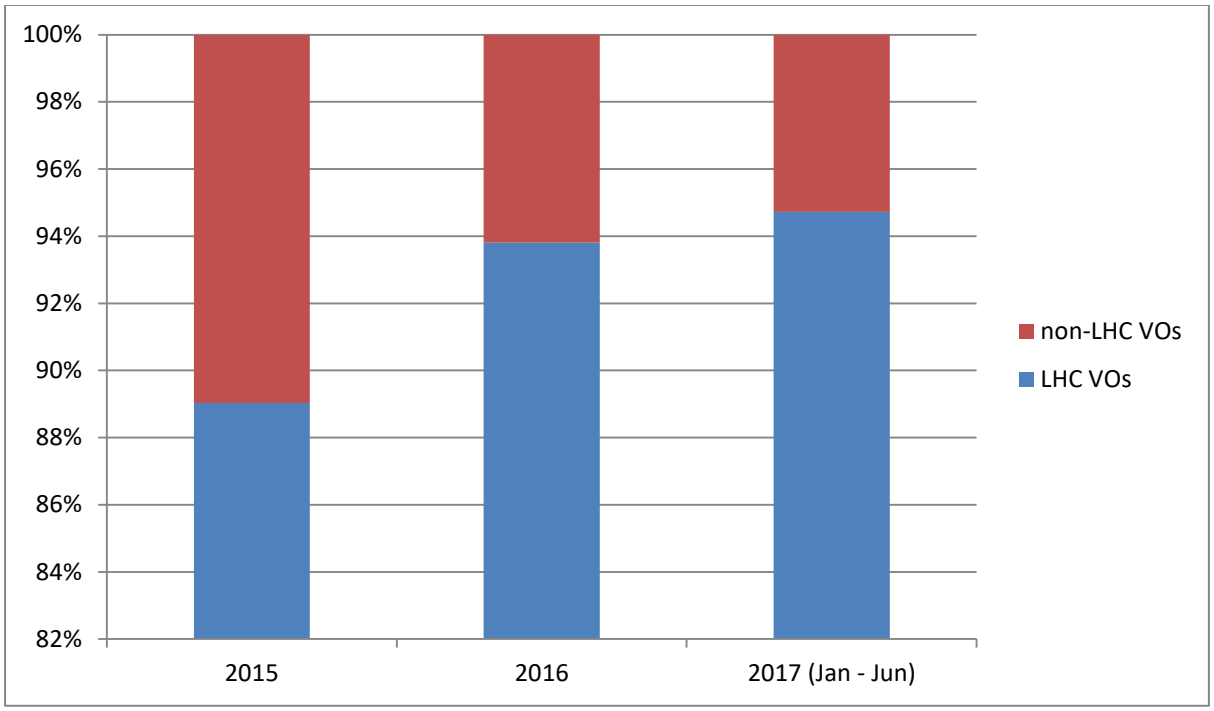


Figure 11: Normalised CPU time usage (%) between LHC and non-LHC VOs over the past years.

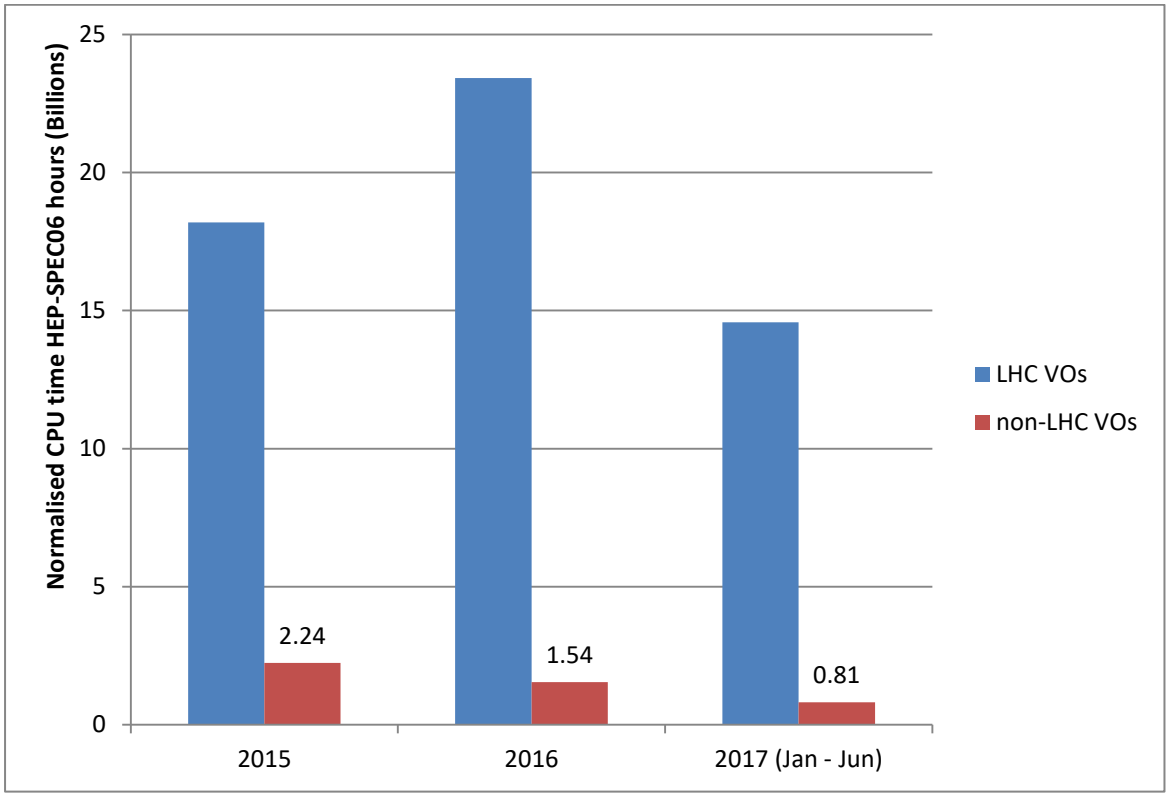


Figure 12: Normalised CPU time consumed by HEP and non-HEP VOs.

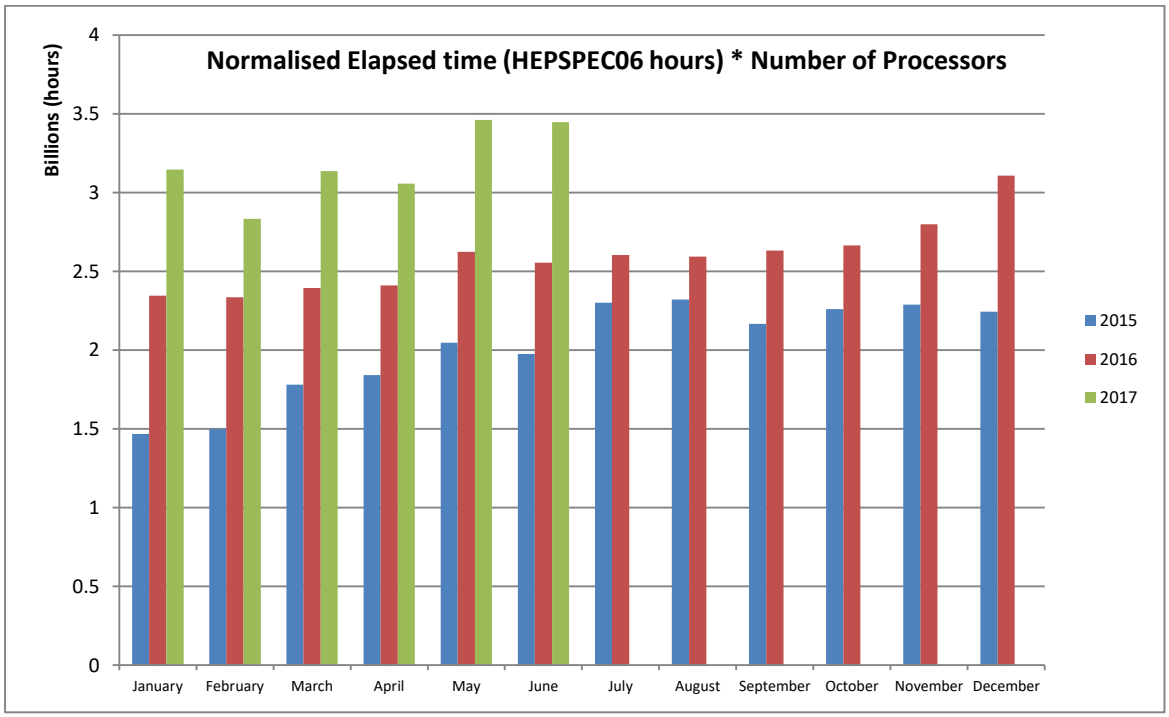


Figure 13: Multicore jobs CPU time. This diagram provides an approximation of the cumulative wall time-equivalent consumption of CPU for multicore jobs.

The accounting of multicore jobs was implemented in production during 2015. This new capability can report accounting information of multi-core jobs, which means that a single computing task is parallelized by running concurrent threads on different cores. As accounting records are accumulated over time, MPI accounting capability will be a more accurate indicator of the amount of parallel computing workload supported by EGI, and will also complement the information about MPI support available in GOCDB and the information system. This being the case, the normalized CPU time consumed by this kind of jobs is reported in Figure 13, which shows how their usage is growth over the past years.

2.2 Cloud resources

The EGI Federated Cloud is part of EGI infrastructure: it is a seamless network of academic and private clouds and virtualised resources, built around open standards and focusing on the requirements of the scientific community. The Federated Cloud is targeted at researchers and research communities that need to access digital resources on a flexible environment, and it currently federates OpenStack, OpenNebula and Synnefo technology based clouds, and allocates them for scientific research and education. The common interfaces provided to access the virtualized resources are Open Cloud Computing Interface (OCCI) and Cloud Data Management Interface (CDMI).

Cloud resources support the Cloud compute and cloud container compute services of the EGI catalogue.

In July 2017 the resource centres joining the EGI Federated Cloud, offering a Cloud Compute capability, are 24, as shown in Table 3, which reports also the cloud management framework provided by each site together the number of cores and the amount of disk space declared.

Table 3: EGI cloud providers (July 2017)

Resource Centre	NGI	Number of cores declared	Amount of disk space declared (TB)	Cloud Management Framework
100IT	NGI UK	120	16	OpenStack
BEgrid-BELNET	NGI_NL	160	10	OpenNebula
BIFI	NGI IBERGRID	720	10	OpenStack
CESGA	NGI IBERGRID	448	3,7	OpenStack
CESNET-MetaCloud	NGI CZ	416	56,6	OpenNebula
CETA-GRID	NGI IBERGRID	184	5	OpenStack
CLOUDIFIN	NGI_RO	96	2	OpenStack
CYFRONET-CLOUD	NGI PL	200	5	OpenStack
FZJ	NGI DE	216	50	OpenStack

GoeGrid	NGI DE	192	40	OpenNebula
HG-09-Okeanos-Cloud	NGI GRNET	70	2	Synnefo
IFCA-LCG2	NGI IBERGRID	2368		OpenNebula
IISAS-FedCloud	NGI SK	168	9	OpenStack
IISAS-GPUCloud	NGI SK	48	6	OpenStack
IISAS-Nebula	NGI_SK	32	0,147	OpenNebula
IN2P3-IRES	NGI FRANCE	480	45	OpenStack
INFN-CATANIA-STACK	NGI IT	16	16	OpenStack
INFN-PADOVA-STACK	NGI IT	144	4	OpenStack
MK-04-FINKICLOUD	NGI MK	100	1	OpenNebula
NCG-INGRID-PT	NGI IBERGRID	80	3	OpenStack
RECAS-BARI	NGI IT	300	50	OpenStack
SCAI	NGI_DE	128	20	OpenStack
TR-FC1-ULAKBIM	NGI TR	168	40	OpenStack
UPV-GRyCAP	NGI IBERGRID	128	5	OpenNebula

The cloud resources usage, in terms of VMs instantiated and CPU time (not normalised) consumed, is reported in Table 4. The higher numbers scored in 2015 are due to an intense activity of the ATLAS VO concentrated in some months of testing the cloud paradigm, as can be seen in Figure 14 and in Figure 15 where it is pictured the monthly usage, where in the first months of 2015 there are the higher bars of the graph. The tests for the ATLAS vo have not continued after 2015

Table 4: EGI Fedcloud usage over the past years

Cloud usage during:	2015	2016	2017 Jan-Jun (increment)
Total # of VMs instantiated	412961	296000	179443 (+5.75%)
Total not normalised CPU time consumed (Millions CPU hours)	1.65	1.43	0.55

In Figure 16, Figure 17, and Figure 18 it is plotted the percentage of not normalised CPU time consumed by VO during the years 2015, 2016, and 2017 (first six months) respectively. The catch-all VO fedcloud.egi.eu scored the largest consumption, and it is evident the great activity performed by the atlas VO during 2015, as written above, disappeared in the next years.

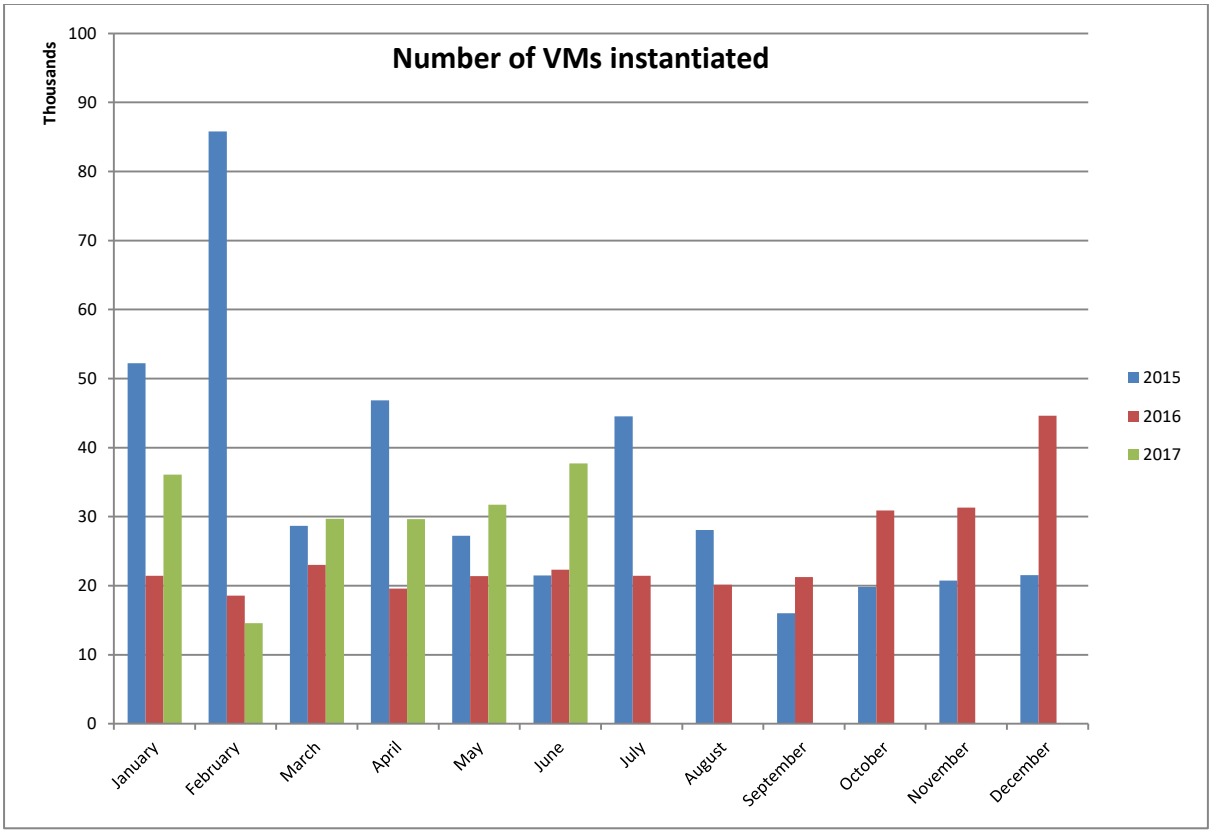


Figure 14: Number of VMs instantiated by the EGI FedCloud providers.

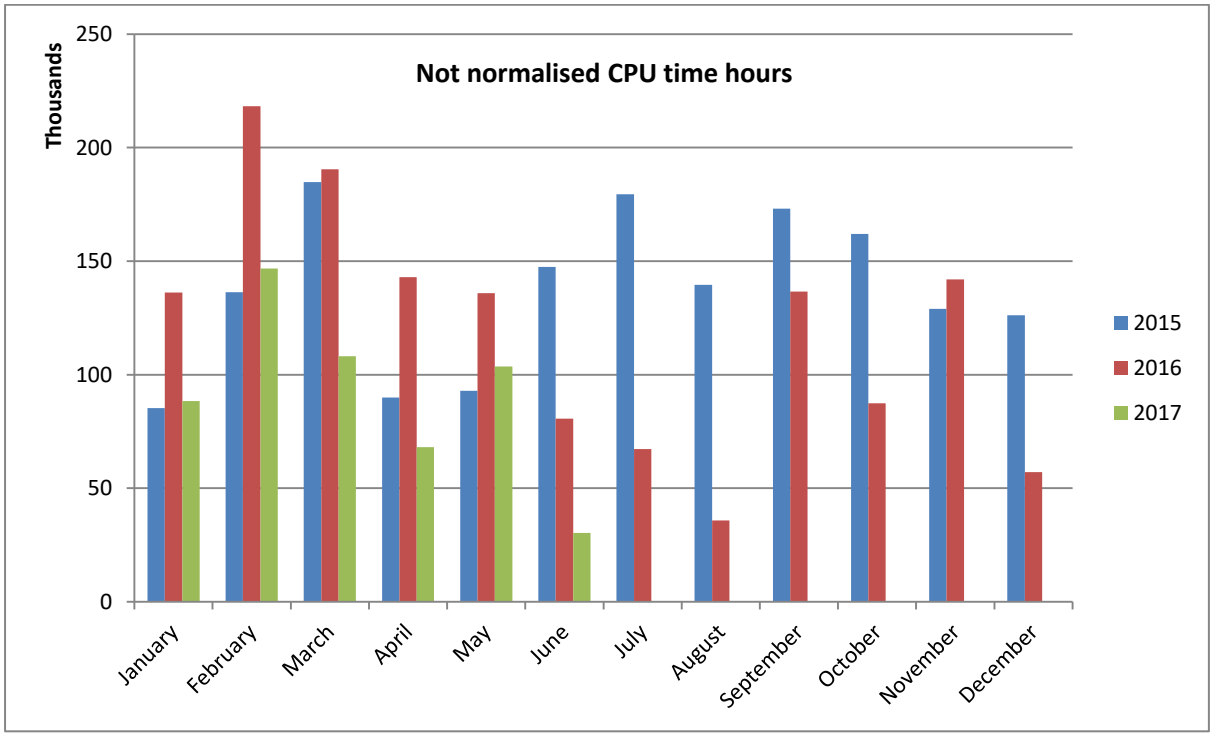


Figure 15: not normalised CPU time consumed in the EGI FedCloud.

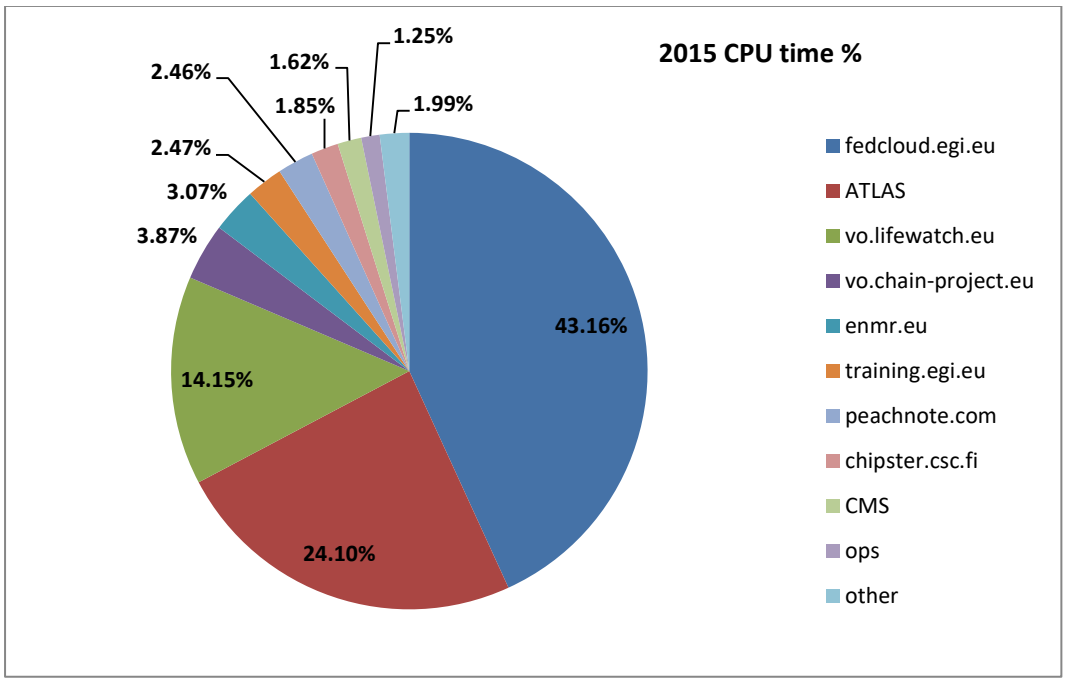


Figure 16: not normalised CPU time (%) by VO consumed in 2015

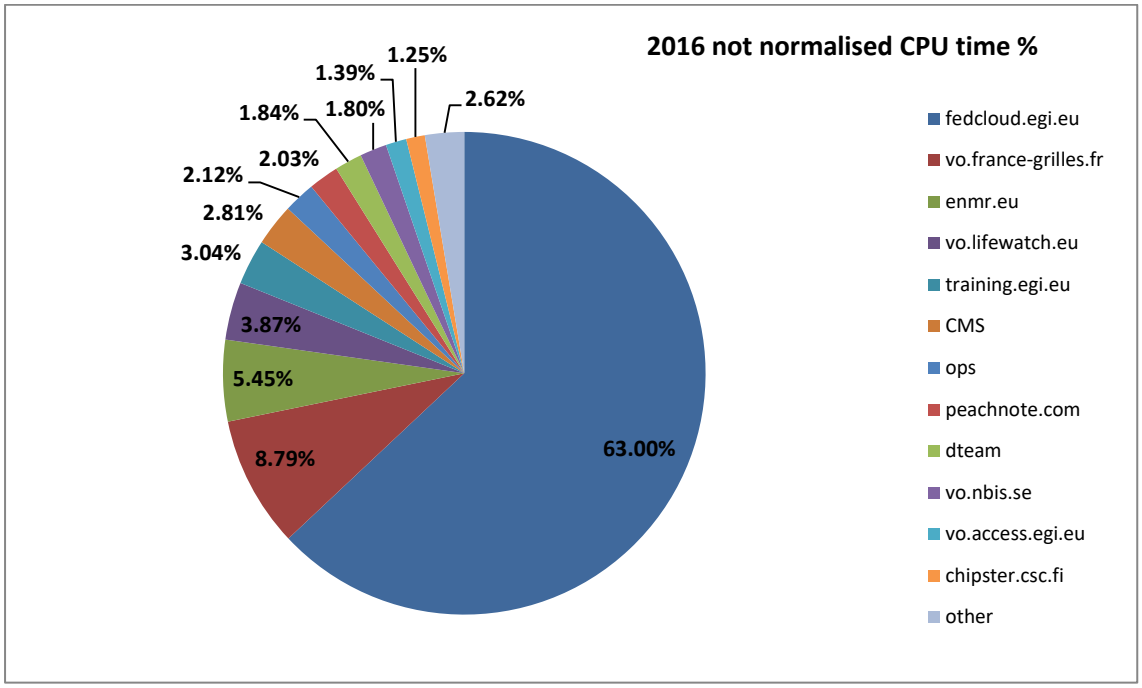


Figure 17: not normalised CPU time (%) by VO consumed in 2016

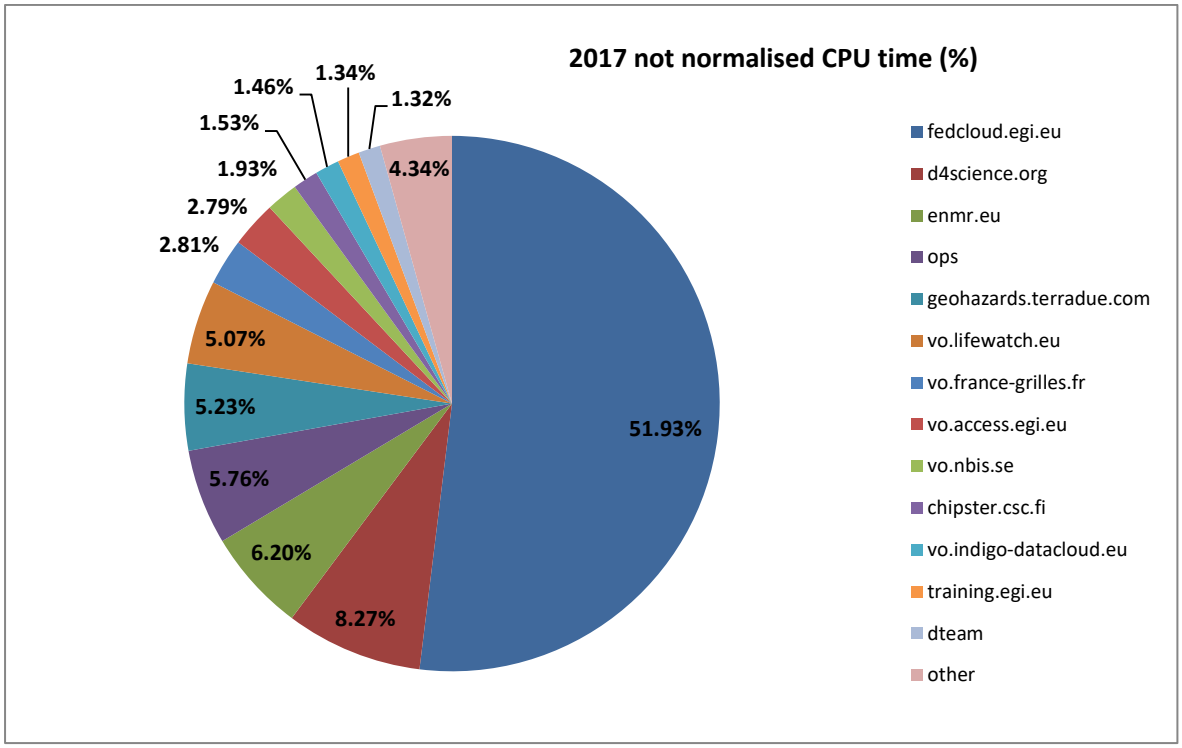


Figure 18: not normalised CPU time (%) by VO consumed in 2017 first-half

The decrease in percentage usage of cloud resources by the fedcloud.egi.eu catch-all VO, which is an incubator VO for new use cases or small use cases, (63% in 2016, 52% in 2017) shows that cloud the use cases are consolidating, moving their users from the catch-all VO to dedicated VOs with dedicated VO SLAs.

2.3 Storage resources

The Storage Management capability is defined as that technology that 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 EGI three data management platforms are available: DPM, dCache and STORM.

Storage resources support the "Storage and Data" services of the EGI catalogue.

The total amount of storage certified service endpoints is 270, which corresponds to a total disk capacity of about 299.2 PB, recorded in July 2017 (Figure 19). In February 2016 the total disk capacity reported was 264.18 PB, so it increased by 13.27%. On the other hand the total tape capacity (also called nearline storage), which is mainly provided by CERN and WLCG Tier-1 RCs amounts to 346.4 PB. In February 2016 the corresponding value was 239.8 PB, so the increase was 44.46%.

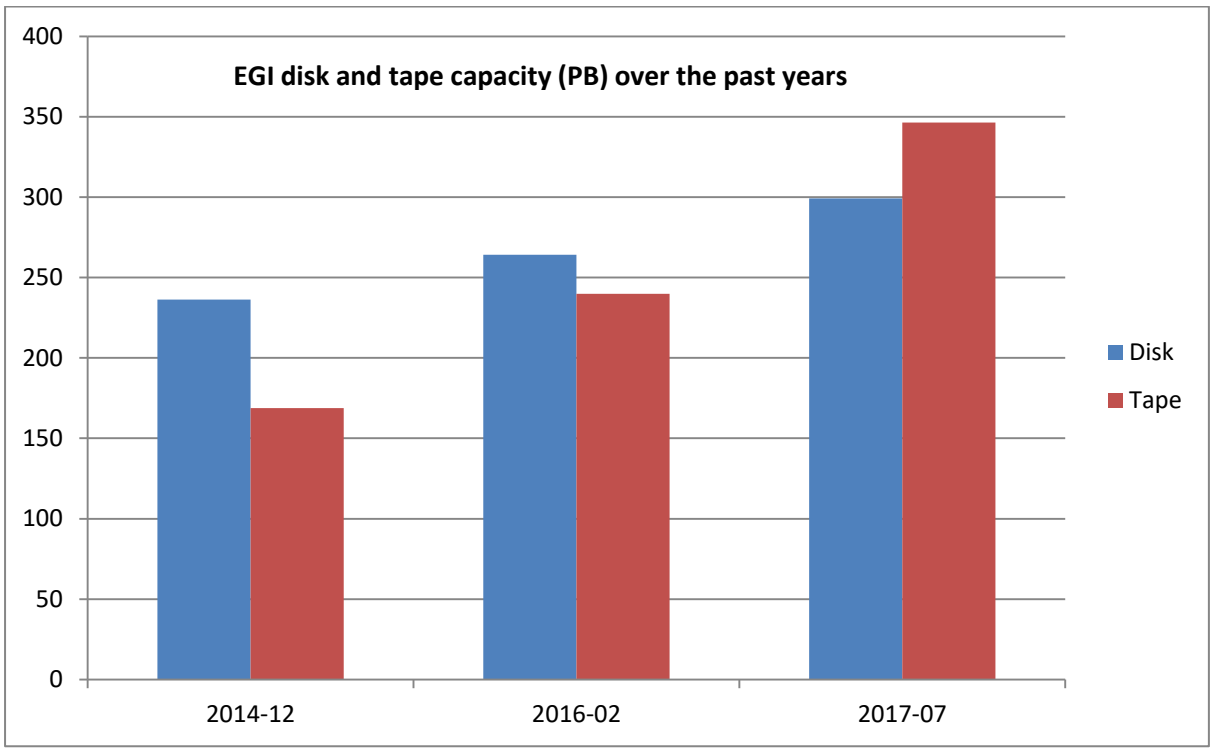


Figure 19: EGI storage capacity over the past years

The distribution of disk storage resources among the EGI operations centres is shown in Figure 20, which shows that the disk capacity is concentrated across six NGIs: NGI_DE, NGI_UK, NGI_IT, NGI_FRANCE, NGI_NDGF, and the Asia-Pacific region, in descending order. Most operations centres maintained the storage capacity in the last six months, with the exception of NGI_DE where in several sites there was an increment of the installed capacity.

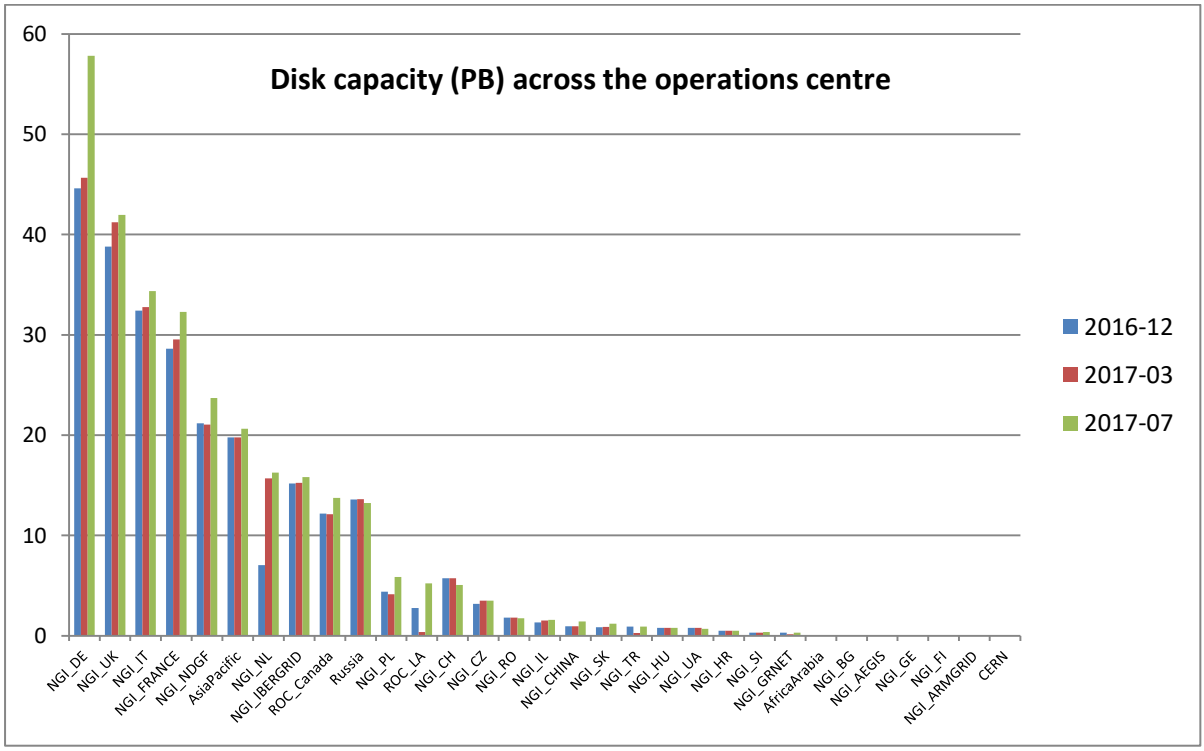


Figure 20: Disk capacity across the OCs over the last few months

The operations centres that contribute to the infrastructure tape capacity are shown in Figure 21, which also highlights the remarkable increase of the resources provided by NGI_FRANCE registered during the last few months.

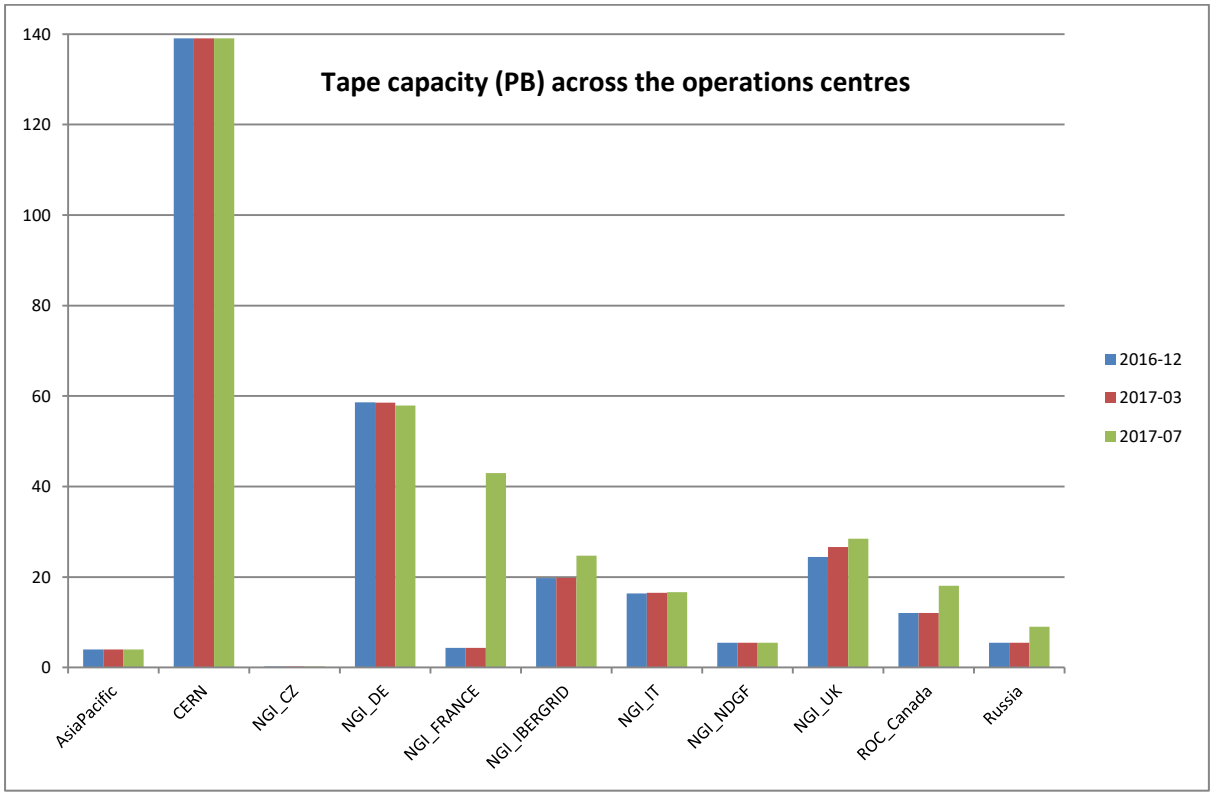


Figure 21 Tape capacity across the OCs over the last 8 months (source: VAPOR).

2.4 Users and communities

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]. We should keep in mind that users have different ways of authenticating when accessing services in the distributed infrastructure (e.g. via credentials released by the home organization, personal certificates, and, in the future – where possible – via social network accounts like google LinkedIn and Facebook). In addition to this, access can be mediated by platforms or Virtual Research Environments which provide customer-specific tools and services, while relying on baseline e-Infrastructure services. Because of this complexity, the number of active users can only be estimated.

The overall number of international and national projects (also known as Virtual Organizations) registered in the Operations Portal[10] at the beginning of July 2017 amounts to 242.

[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.
[10] https://wiki.egi.eu/wiki/Scientific_Disciplines

2.4.1 Robot certificates

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 a 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 July 2017 the number of robot certificates embedded in user gateways is 189 and they are used by 58 VOs in total. About 13000 users can potentially use scientific gateways. This is increased by the number of registered users to active VOs, which amounts to be 30502 in July 2017.

The diagram in Figure 22 shows the trend in use of robot certificates and VOs since November 2011. The increase in the number of Robot Certificates indicates that users, in particular new user communities, are looking for alternative authentication mechanisms different from the plain X.509 certificates.

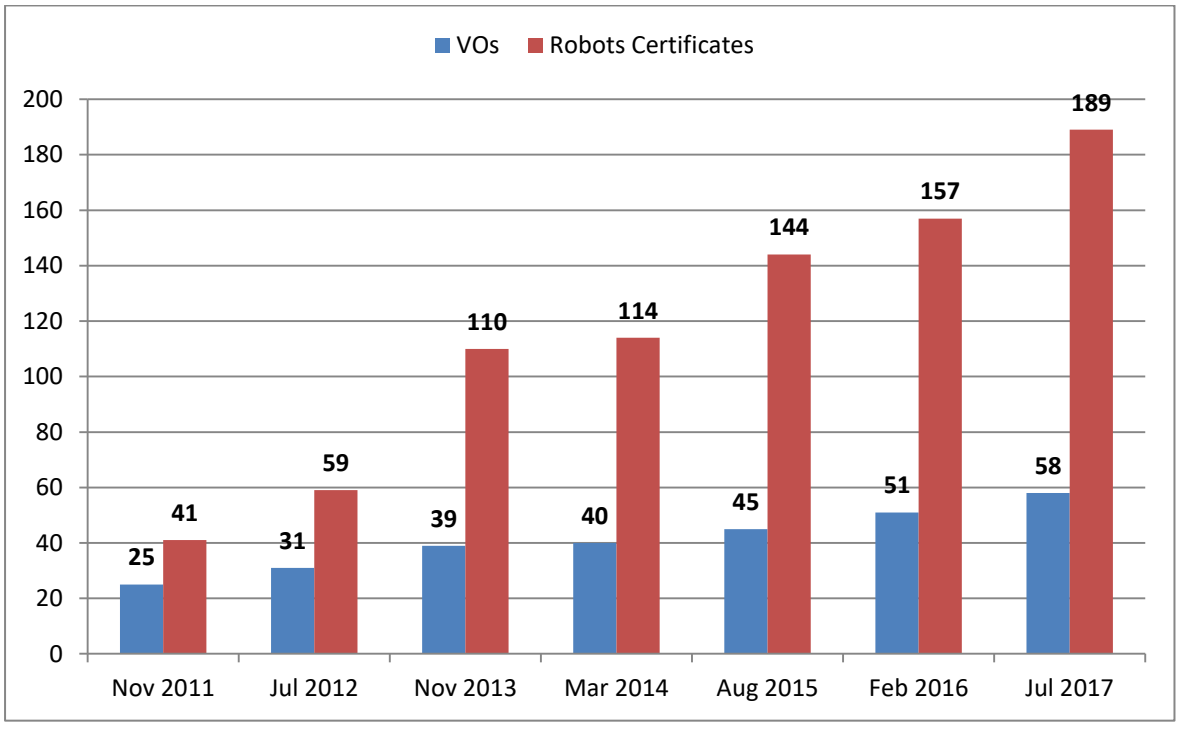


Figure 22: Use of robot certificates and related VO in EGI since 2011.

In Figure 23 we can see how the robot certificates are distributed among the VOs.

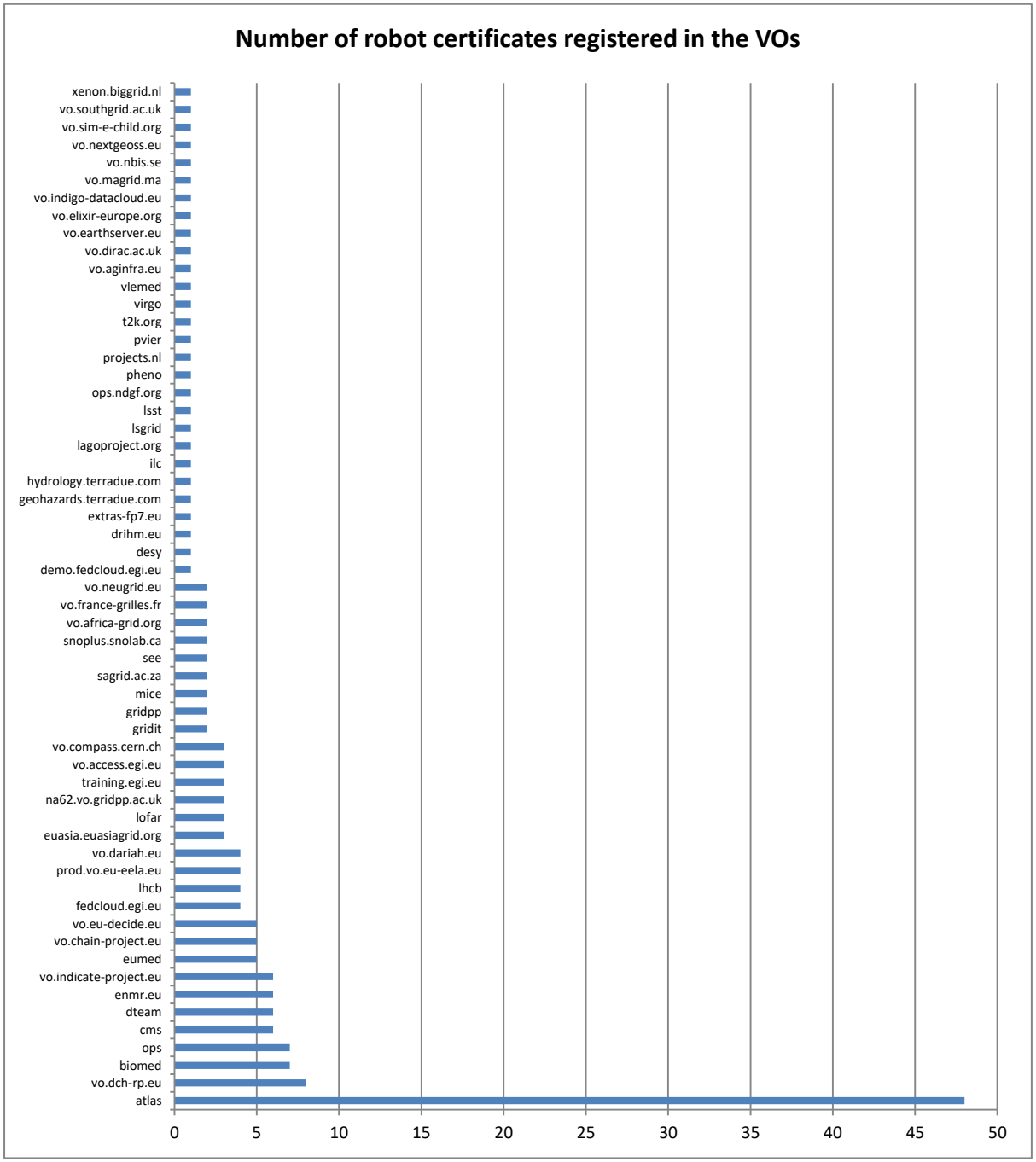


Figure 23: Distribution of robot certificates in the VOs.

2.4.2 VOs and user distribution across scientific fields

Figure 24 shows the VOs distribution in each discipline. The information in this section is based on the disciplines classifications available in the EGI wiki[11], VO can support multiple disciplines based on the use cases supported.

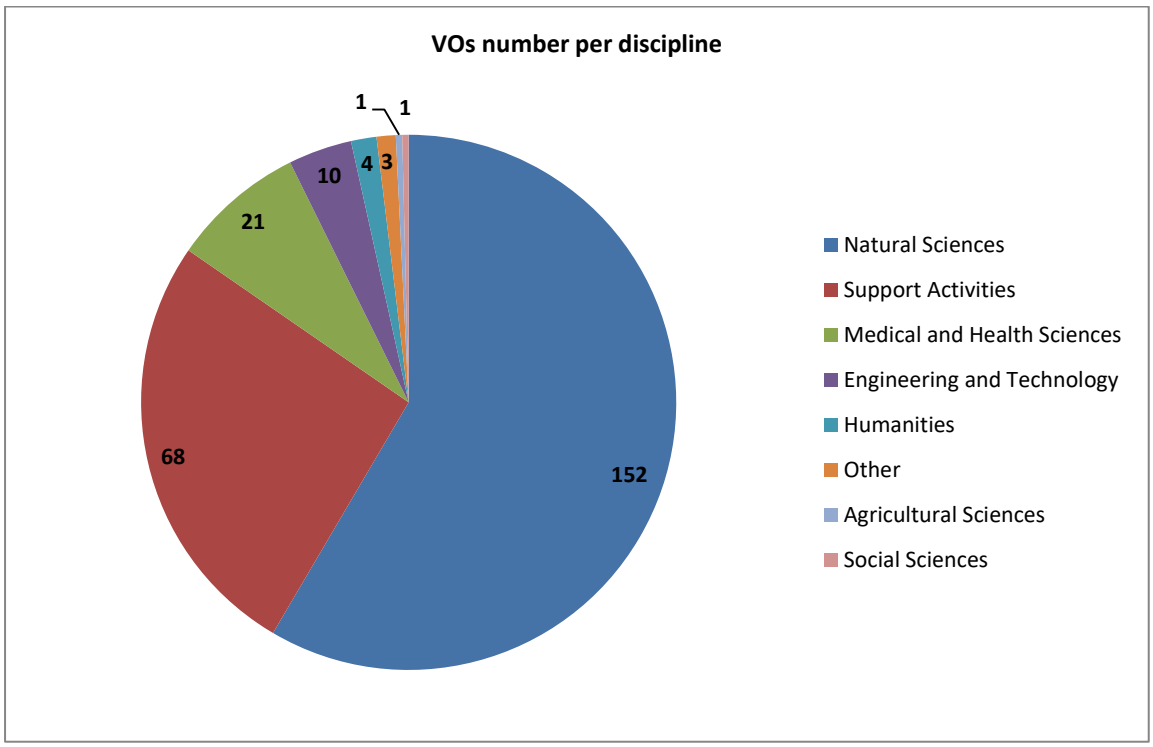


Figure 24: VOs number per discipline (July 2017, source: Operations Portal).

The largest discipline in terms of number of registered users is Natural Sciences (78.01%): it is remarkably larger than the other ones because it includes 152 VOs (more than the half of the total VOs). Then there is the Support Activities discipline (13.89%), followed by Medical and Health Science (5.55%) and by Engineering and Technology (1.18%). The complete users' distribution is shown in Figure 25. Please note that in these numbers each VO can be associated to one or more disciplines sub-categories.

[11] https://wiki.egi.eu/wiki/Scientific_Disciplines

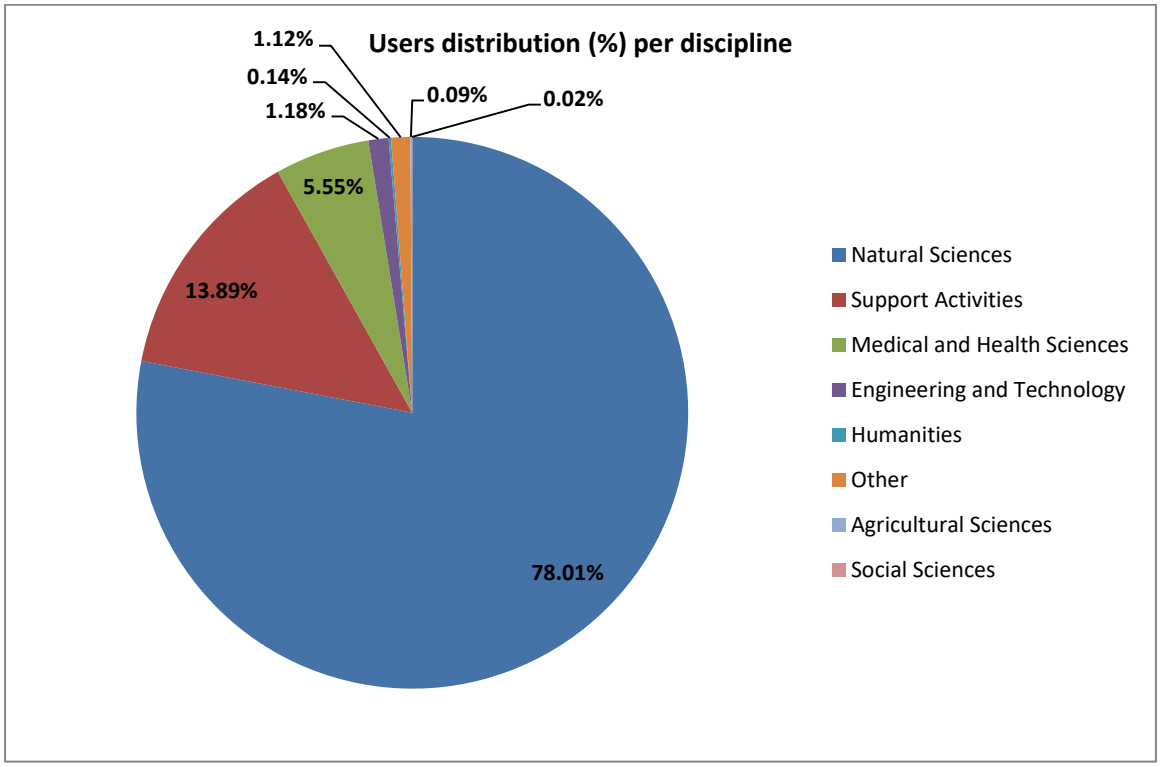


Figure 25: Users distribution per discipline (July 2017, source: Operations Portal).

2.4.3 Resources usage by disciplines

Table 5 reports on the increase or decrease in HTC resources usage (in terms of HEP-SPEC06 hours consumed) in 2016 and first half of 2017 by the scientific disciplines.

Table 5: Relative increase/decrease of normalised CPU time utilization (HTC resources) in 2016 (compared to 2015) and in first half of 2017 (compared to 2016 second half), ordered by 2017 utilization (source: accounting portal).

DISCIPLINE	2016 increment	2017 increment
Natural Sciences	26,39%	15,58%
Medical and Health Sciences	-57,60%	5,35%
Support Activities	-12,30%	-45,92%
Engineering and Technology	-36,65%	-9,05%
Agricultural Sciences	-100,00%	n.a.

In Table 6 there is an highlight of the 10 most active sub-disciplines in EGI.

The largest discipline, Natural Sciences, is continuing to increase the infrastructure utilisation: the first 8 subdisciplines in terms of resources usage are all belonging to it. The subdiscipline Medical Imaging (Medical and Health Sciences), mainly leaded by biomed and vlemed VOs, had a remarkable decrease in 2016, while in the first half of 2017 showed light signals of growth: the support of one of the vlemed science gateways was discontinued in 2016 for a funding reduction, so the users activities were affected; biomed instead, given its nature of catch-all VO, has usually got fluctuations in the activities due to variations in computational needs of the served research communities. The same fluctuation can explain the decrease scored by Computational Chemistry in the first 6 months of 2017, compared to the normalised CPU time consumed in the second half of the previous year. The support Activities discipline is a collection of testing and training VOs: the main users are developers, NGIs operators, and RCs administrators, the usage is dedicated to debugging issues and testing the infrastructure in general. The Agricultural Sciences discipline stopped completely the activities since 2016.

Table 6: Relative increase/decrease of normalised CPU time utilization (HTC resources) in 2016 and in 2017 (first half), ordered by 2017 utilization (source: accounting portal).

Sub-discipline	increment 2016	increment 2017
Physics	27,31%	16,15%
High energy physics	23,56%	15,28%
Particle physics	17,49%	22,64%
Nuclear physics	19,27%	22,22%
Astrophysics	51,28%	17,99%
Space science	52,60%	17,89%
Astronomy	53,57%	21,66%
Accelerator physics	63,17%	-33,43%
Medical imaging	-58,43%	4,89%
Computational chemistry	18,79%	-30,82%

Table 7: Relative increase/decrease of not normalised CPU time utilization (cloud resources) in 2016 and in 2017 (first half), ordered by 2017 utilization (source: accounting portal).

Discipline	increment 2016	increment 2017	2017 Jan/ Jun (hours)
Support Activities	88,77%	-48,03%	415k
Natural Sciences	-79,41%	-16,02%	101k
Engineering and Technology	1524,70%	785,24%	36k
Medical and Health Sciences	154,26%	415,02%	9k
Humanities	-25,95%	-99,96%	6

Regarding the FedCloud resources utilisation, the main disciplines are Support Activities and Natural Sciences, both disciplines scored a decrease in the last year. In the first one the decrease is due to the catch-all VO fedcloud.egi.eu, whose resource usage fluctuates over the months and the years being an incubator VO for new use cases, while the second one because the reduction in the fedcloud activities of the LHC experiment VOs. "Engineering and Technology" and "Medical and Health Sciences", still producing lower accounting data than the predominant, are remarkably increasing their usage, very likely the VO SLAs framework agreed with the resource providers (see section 5). "Humanities" has almost stopped their activities.

3. Federated and NGI/EIRO operations

During July 2017, EGI Operations run a survey among the operations centre, to collect information about the current status of national operations and the plans up to the coming three years. The results of the survey have been used as inputs for this document, together with other feedback from the Operations Centres. More details on the results are provided in the following sections.

The survey's questions focused on the following topics:

- Sustainability of the operations centres activities. The current sources of funding and the expectations for the future.
- Interaction with the central operations. Where the collaboration between EGI and Operations Centres operations should strengthen in the coming months.
- Services provided for the user communities. Current service portfolio and the areas where service provisioning will focus at national level.

The survey received 15 answers, which although a quite limited subset of the total operations centres, had a good distribution of answers between small, medium and big national initiatives.

3.1 National and EIRO Operations Centres

High throughput computing is still the most used service in the EGI federation, about 90% of the federated resource centres are providing compute and storage services, to support HTC users. It is clear that the large majority of the resource centres, and consequently operations centres, will continue to provide HTC services to support their users.

New services and new technologies are gaining popularity among the new users and new collaborations, making increasingly important that the OC support the resource centres in the provision of a wider service portfolio. This activity needs to be supported by sufficient effort at national level to coordinate the operations of resource centre level.

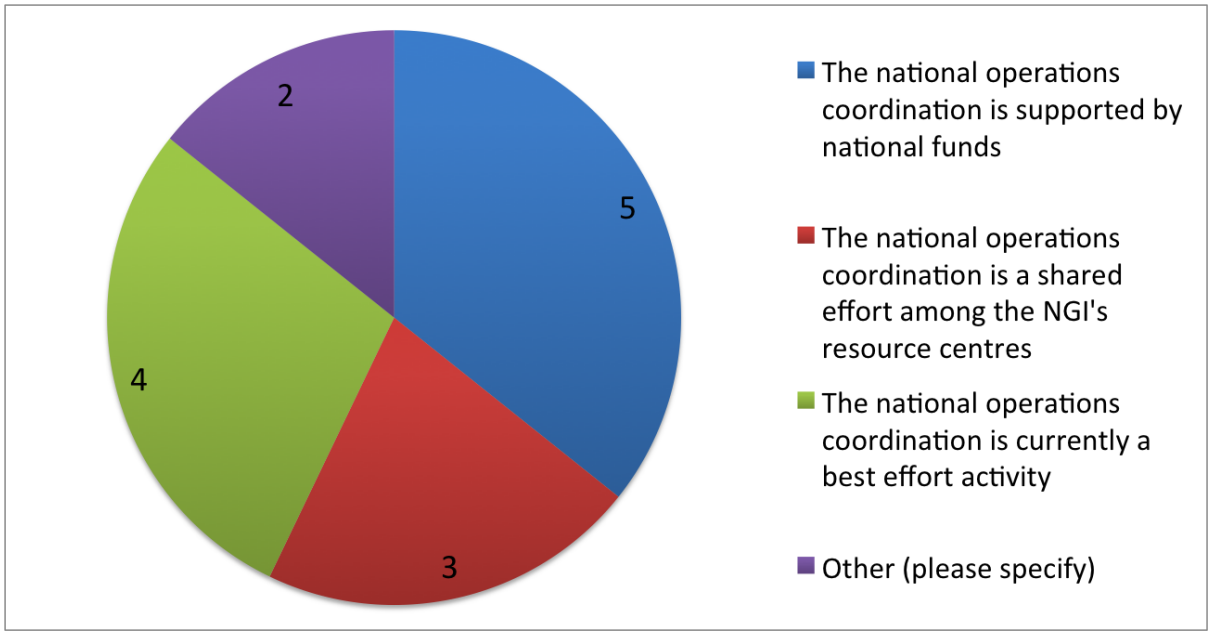


Figure 26: 2017 Survey, current funding available for the OC operations

As shown in Figure 26, the majority of the operations centres participating the survey is supported either by national funding or has an agreement among their resource centres to collaboratively participate to the national operations (8 out of 14), while the minority of the OC answered that their activity is a best effort (4 out of 14). In other words, the majority of the NGIs and EIROs have their operations run in a structured way.

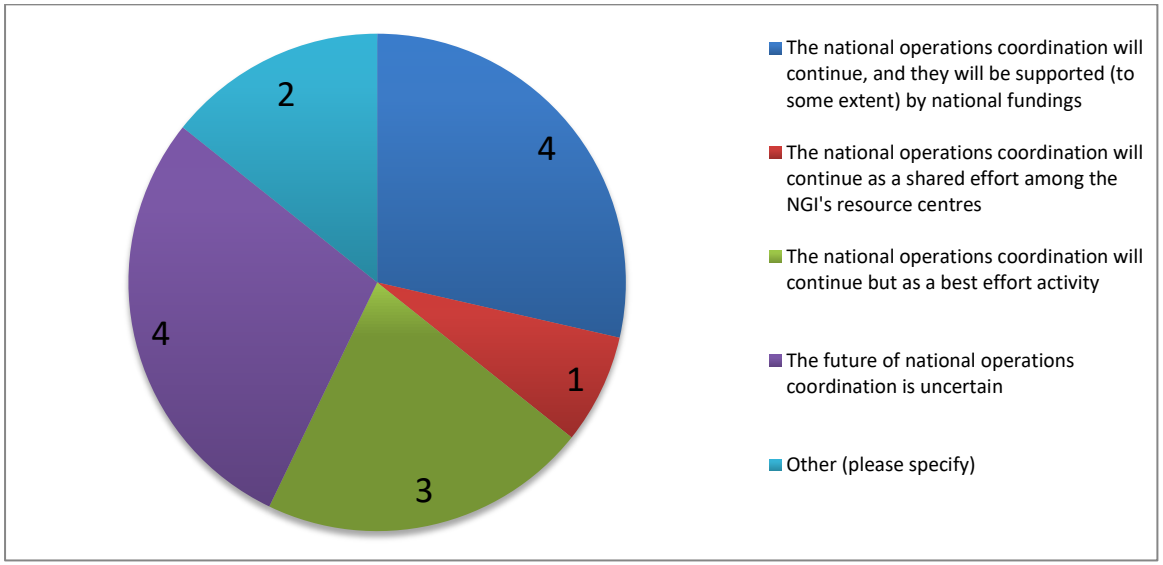


Figure 27: 2017 survey, funding available for the OC operations in the coming 36 months

Figure 27 shows the answers provided for the future funds available to support the operations of the operations centre, in the time period 2018-2020. For the future some NGIs are facing uncertainty, 4 out of 14 answered that there is no certainty that it will be possible to secure effort to support the coordination of national operations. This is an issue that requires to be closely monitored, in particular when affecting medium or big NGIs.

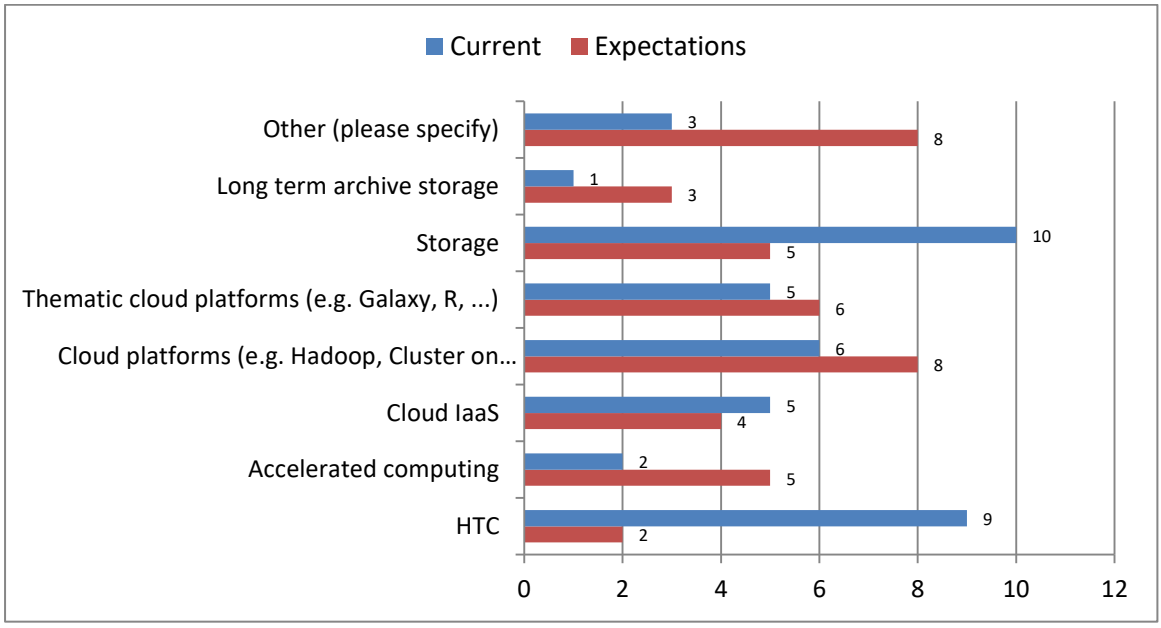


Figure 28: 2017 Survey, service provision. Current priorities and areas expected to grow in demand

Figure 28 shows the results of two questions about service provisioning. What are the services currently important for the existing user communities, and the services on which it is important to invest to support the future requests of the user communities in the coming three years.

HTC and storage services are, at the moment, largely the most important services provided to the EGI users, with their consumption led by the HEP communities, as described in section 30, closely followed by the cloud IaaS.

The general trend extrapolated from the data in the survey for the future 24/36 months is to invest more on cloud and new services types. The initial assessment with the survey has been confirmed by further discussions with the NGIs, for example in the discussion about the results of the survey at the Operations Management Board in July 2017[12].

The technology roadmaps are driven by the fact that the new use cases proposed by the new communities approaching the national resource providers are mostly requesting either IaaS or more advanced services, such as platforms or software as a service. It is already relatively common among EGI communities to have their science gateways or application workflows deployed on EGI resources, and in some cases managed by the resource centres themselves; the scenario is

[12] https://indico.egi.eu/indico/event/3239/

changing since the high-level services that are increasing in demand are not community-specific anymore, but general-purpose or specific to a wider domain, off-the-shelf platforms and solutions. Examples of these advanced multi-community services are: Galaxy, Hadoop/Sparks, and Jupyter. These high level services have the potential to be used by several different communities for different use cases.

At the moment the coordination for the exploration of new services by the operations centres and resource centres is at national level, and very limited at infrastructure level. Increasing the coordination at infrastructure level is considered high priority for the operations centres, the coordination action would not aim at steering the national roadmaps, but it would focus on:

- Increase international visibility to the services
- Exchange experiences and know-how among the NGIs and EIRO about service provisioning
- Enable access to the existing services to international virtual organisations

3.2 Federated operations

The plans and strategy of the national resource providers will be reflected also in the operations coordination at federation level. The operational processes and procedures will evolve to be compatible with new services and new operational activities at NGI and EIRO level.

The survey had two questions dedicated to the central operations:

- How can central operations better support the national operations
- How should central operations evolve, more in general

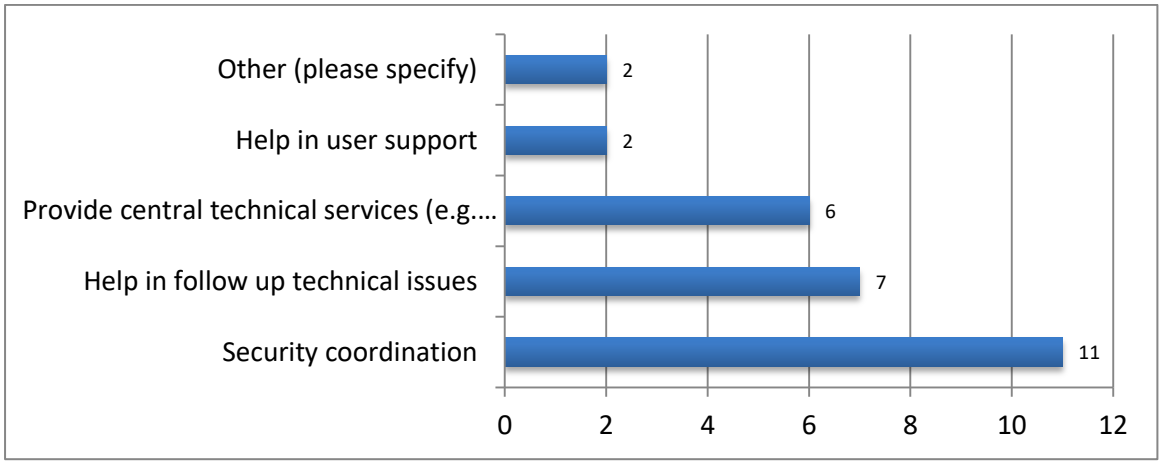


Figure 29: 2017 Survey, Where can central operations support national/EIRO operations?

The figure above shows the areas identified in the survey where EGI Operations should support the national operations.

Security coordination. This is already a very strong and mature activity centrally coordinated by EGI, and supported both by projects and core activities. The operations centres see security

coordination critical, and this can be interpreted also as a consequence of the rapid technological evolution foreseen in the service provisioning: new services may bring also new security threats that will have to be analysed and mitigated in order to maintain the EGI Infrastructure secure and reliable. More information about the evolution of security in section 3.3.

Support in following up technical issues. EGI is centrally supporting the technical issues by providing 2nd level support as a core activity. This reduces the impact of ticket management on the operations centres.

Operations centres have to support the resource centres in case of technical issues that cannot be solved autonomously by the computing centre staff, mainly regarding the interoperation with the federation layer of EGI. Prompt solution of technical issues is critical for providing good quality services, and central operations can increment the effort on complementing the operations centres in supporting the resource centres.

Provide centrally operated services. Users may need services to be used on multiple sites, for example brokers or workload management tools. Providing centrally these services may have multiple advantages: reliving operations centres of the burden of operating dedicated services, select the better technologies to implement the service, and ensure high-standards of the service operations. One example of this support activity is the DIRAC4EGI service, the centrally managed instance of the workload management tool that has replaced, as main solution suggested by EGI, glite WMS.

New technologies and new services may expand the support tools that can be used by the users, for example cloud brokers or platform orchestrators, and a continuous discussion should be active among central operations, operations centres, and community support to identify the services that can improve the user experience and that would benefit from being provided centrally. These activities can be supported as core services (therefore partially funded by EGI fees) or by future projects.

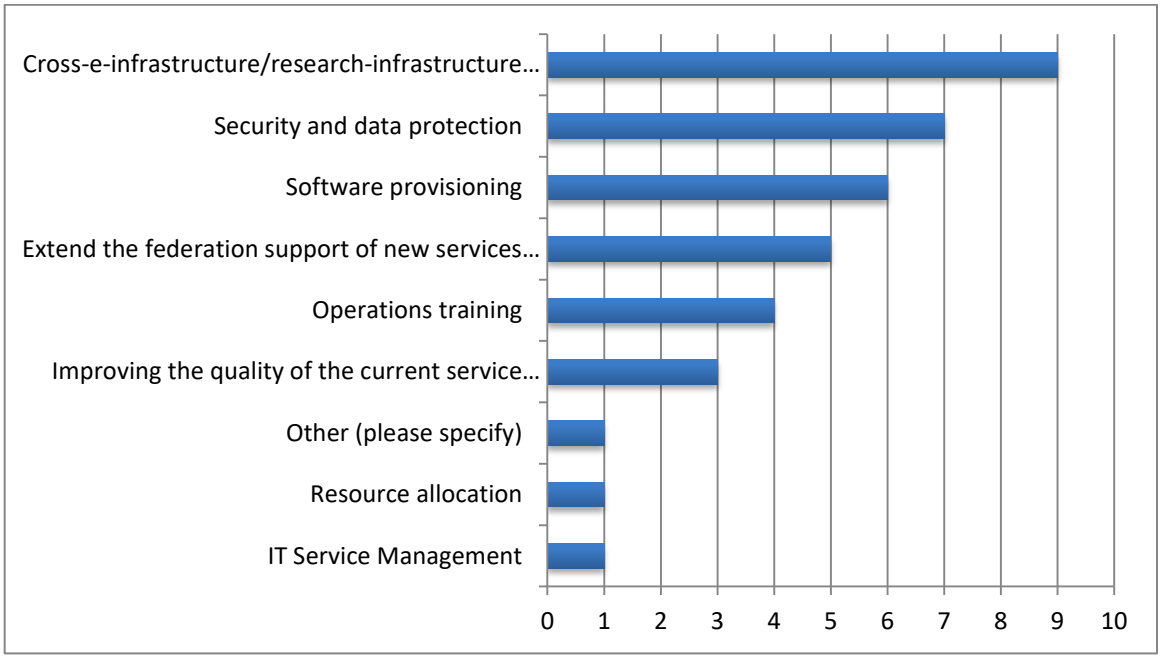


Figure 30: 2017 Survey, Which are the areas where the EGI Federation operations should develop

In the survey the operations centres where asked to list the major areas of future development for the central operations. The answers are summarized in Figure 30, the survey participants were not asked to identify lacks in the current operations coordination activities, but mostly to identify the areas that will increase in relevance in the future months.

Cross e-Infrastructure coordination has been identified as the most important activity to expand in the coming months. EGI has been collaborating with the other e-Infrastructures to improve the interoperability and better support communities using services provided by multiple infrastructures, for example in the context of the AARC project. To further expand these activity EGI operations will collaborate even closer with the other e-Infrastructures, and in particular with EUDAT since the two service catalogues are mostly complementary and communities will benefit of the increase interoperability. In terms of operations coordination, the areas of interoperability of major relevance are: user support, security, and AAI. These topics will be tackled both in future co-participated projects

Security coordination will be discussed in section 3.3 and software provisioning in section 4.1.

The other important requirement is to extend the federation services and procedures to expand the service portfolio. This is a direct consequence of what discussed in the previous section (3.1), new communities are asking for high level services and platforms, and the provisioning of these must be integrated with the EGI federation procedures and core services.

The Operations Management Board will increase the meetings dedicated to new services and in particular the services considered high priority, in order to share the experiences and know how developed by the resource centres and operations centres.

The integration of services will have to be prioritized, for example based on the popularity among users and the re-usability by different use cases. At the moment EGI coordinates the technological evolution with the TCBs (Technology Coordination Boards), but there is no TCB dedicated to the high level services and platform. Although the discussions on new services most probably will initiate at the OMB, it will be ultimately moved in a dedicated TCB.

The services that will be identified as relevant for the infrastructure will have to be processed with the procedure for the operational integration of new middleware[13] that includes, among the other activities:

- Registration the new service in the configuration database (GOCDB)
- Monitoring support
- Implementing accounting data integration
- Security evaluation of the service
- Identification of the main technical contacts for the service

EGI Operations will focus on making faster the integration process.

Another area of development of EGI Operations, in collaboration with other activities such as user support, is the follow up with communities who are decreasing the usage of EGI resources. Resource usage by one user community may have fluctuations over the months, due for example to unevenly spread research deadlines, or may decrease constantly over longer periods of time. The reasons for a consistent decrease may vary, some examples are:

- End of a research project, and consequent dissolution of the community
- Technical evaluation of the EGI services for the community use case ended and the community decided to not continue the use of the services
- The VO is loosely managed, and without a proactive dissemination activities, the number of new users low compared to the leaving users
- The VO does not have the resources to support the technical tools to enable access to the EGI resources for the community's users, nor to provide technical support

For some of these causes of usage decrement EGI federation could proactively support the community trying to retain their users.

One plan under discussion is to monitor medium-big virtual organisation and consistently get in contact with the VO management in case of consistent drop of usage statistics, to understand the causes behind the drop. Where support may be effective to increase VO usage, EGI could provide:

- Technical support and outreach support to new users
- Technical services operated on behalf of the community to enable EGI usage by the users

Again, this plan is under development, since there is need to ensure resources to support such activities.

[13] https://wiki.egi.eu/wiki/PROC19

3.2.1 Core activities

Core activities are the technical services and human activities, mostly operational, that are provided by the EGI Foundation and their partners for the members of the infrastructure to enable the EGI federations and the daily provisioning of the services to EGI customers. The list of the core activities is approved by the EGI Council and then provided in cycles of two or three years. There are processes to add new services during the cycle, in this way EGI federation can be agile to answer to new requirements.

Once the list of core activities to be funded is defined, EGI operations prepare a detailed description with the technical requirements for every one of this activity and it is made available to the EGI council members. EGI Council members interested to participate in the core activity provisioning prepare an expression of interest, which includes a technical specification of the service they would provide, and all additional information to evaluate the proposal and submit to EGI Operations.

Expressions of interest are then evaluated technically and ranked using the priorities as described in the wiki page dedicated to the bidding process[14]. The service providers selected, for the bid period, in the preliminary assessment are then finally approved by EGI Council.

The funding of the core activities is co-funded by the EGI Foundation and the service providers: a percentage of the allocated effort for the activity is funded by the EGI Foundation, supported by the council fees, and another percentage of the effort is co-funded by the service provider as in-kind contribution to the core activities.

A new bid was run in the last quarter of 2016, to plan the core activities provisioning for the years 2018-2020. The EGI Council approved to support the following services:

Accounting repositories and portal	Operations portal
Message brokers	Security coordination and tools
Monitoring	UMD and CMD quality assurance
Service registry	UMD and CMD software provisioning infrastructure
Helpdesk tools	Services for the AAI
Helpdesk support	Online CA
Collaboration tools (EGI website, wikis, and other tools)	Marketplace
Application DB	DIRAC4EGI

Table 8: Core activities for the period 2018-2020

[14] https://wiki.egi.eu/wiki/EGI_Core_activities:Bidding

The last four rows in the right column of the table above are new services that have been added to the list of core activities, and three of them are outputs of the EGI-Engage project that will be deployed in production with a long-term sustainability plan:

- Services for the AAI are the CheckIn service which has been designed in task JRA1.1, and it is already a beta service in the EGI catalogue. CheckIn will be the AAI platform for the EGI services, and it has been listed among the services to be supported in the medium long term as core activity.
- Online CA is the translation service to X.509 certificates; it is an output of both EGI-Engage and AARC project. This service will support EGI users to access services supporting X.509 authentication with their federated credentials. This service will potentially be operated as part of a multi-infrastructure online CA, supported by EGI and by other e-Infrastructures. A single Online CA in Europe would increase interoperability among service providers, and therefore it is in the users' interest that the Online CA has been designed as a collaborative effort for the future.
- Marketplace is the service currently prototyped in the JRA1 work package, and that will be operated to host the EGI services catalogue and to allow users to submit service orders.
- DIRAC4EGI is the workload management system that allows HTC users to manage thousands of jobs submitted to multiple resource centres form a single entry point. It has been chosen as the main suggested option for workload management system, and therefore it is important to provide at least one instance for the user communities who do not have resources to deploy a dedicate installation.

Service providers for all the services have been identified through the bidding process and the EGI Council has approved the designations in 2016.

3.3 Security coordination evolution

The work done by EGI-Engage SA1/WP5 to evolve the EGI security coordination of operations, policies, procedures and best practices was fully described in Deliverable D5.3[15] Section 8 of that document presented the plans for the last 6 months of the project and these have been addressed since its publication. These include:

- review and revision of the security risk assessment;
- wider deployment of the VM Operator role in the EGI FedCloud service;
- work on risk assessment within the WISE RAW working group;
- review and revision of procedures where needed;
- revision of all VO security policies, replacing these with new "Community" policies;
- development of a process for assessing the combined adequacy of AAI assurance levels;

[15] https://documents.egi.eu/document/3027

- publication and endorsement of SCI Version 2 at TNC17 in Linz;
- further development of the SSC framework and running a FedCloud security challenge;
- updating of SVG processes to adapt to new technology and deployments.

The following sub-sections will focus on the open issues for security and what are the current plans to address them in the coming months.

3.3.1 Ongoing operational security issues beyond the end of EGI-Engage

The evolution of operational security must of course continue beyond the end of the EGI-Engage project, security must be an ongoing, non-static, process. EGI will still enable new modes of delivering its services to a growing community of users with new trust models and new mechanisms of identity management. The EGI security team must therefore continue to develop and implement the policies and procedures required to ensure consistent and coordinated security operations across all the services provided in the catalogue. Security across distributed service providers must be based on an up-to-date policy framework and all new policies and procedures should complement the security best practices implemented by the individual service providers. Security policies, procedures, operations, technology and trust must also constantly evolve to address new security threats and risks as they arise.

The ongoing responsibilities of the EGI security team will include all of its current activities, namely the coordination and steering of the CSIRT/IRTF, SPG, SVG, security monitoring, training and dissemination, and the building of trust and policies related to Identity Management and AAI. Issues related to Data Protection and Privacy must also be addressed, particularly as the new EU GDPR comes into force during 2018. It will be beneficial to EGI to additionally continue our ongoing leadership roles in many external security and trust bodies including IGTF, EUGridPMA, FIM4R, WISE and SCI.

In more detail, the ongoing security issues include:

- **CSIRT/IRTF**. Security coordination must ensure that routine issues and security events are handled properly by all participants in EGI, and must provide specialised expertise in forensics and coordination for large scale incidents that threaten the whole of the EGI infrastructure. The emergence of new usage patterns, more diverse user communities, and diversifying infrastructure will lead to more operational pressure on this area, and the IRTF coordination task can help in engaging specific expertise from trusted experts on demand.
- **The Security Policy Group (SPG).** Appropriate security must be based on an adequate and up-to-date policy framework covering diverse aspects, including operational policies (agreements on vulnerability management, intrusion detection and prevention, regulation of access, and enforcement), incident response policies (governing the exchange of information and expected actions), participant responsibilities (including acceptable use policies, identifying users and managing user communities), traceability, legal aspects, and the

protection of personal data. Security operations must coordinate the SPG and ensure engagement with peer infrastructures through WISE, and with identity providers through liaison with and support of the IGTF and EUGridPMA and through engagement with the REFEDS community.

- **The Software Vulnerability Group (SVG)**, must continue to provide coordination for the handling of software vulnerabilities in the new age of highly distributed and more independent providers of software for EGI. SVG's purpose continues to be "To minimize the risk to the EGI infrastructure arising from software vulnerabilities". Central coordination is essential for the consistent handling of vulnerabilities and for sending timely, unambiguous and consistent messages to the EGI resource centres, user communities and partners.
- **Security monitoring** continues to be an important activity. Changes to the infrastructure and service capabilities will necessitate the development of alternative monitoring strategies and incident remediation. Security coordination have identified the requirement for investment in new monitoring and control technology, e.g. in better network monitoring in FedCloud resource providers. Similar work will be needed for any other emerging technology used in distributed infrastructures (be it in EGI or in community services). Current security monitoring would benefit from being extended to a wider security assessment technology that will be able to reflect different needs.
- **Security training and dissemination** remains an important activity. EGI has a well-established portfolio here, with a range of different types of training. Consolidation of this, both in terms of effort and support for travel and subsistence, would allow us to be more effective. Although the EGI security team is well able to coordinate and establish a training regimen, it should be anticipated that for expert-level training there will be a need to involve external trainers, who usually require at least support for their travel costs. An independent funding stream and business model would need to be found to permit external experts to support such advanced training sessions.
- **Trust and AAI.** e-Infrastructures see a growing requirement to develop and maintain trust and policy frameworks which are useful to the broadest possible range of e-Infrastructures and Research Infrastructures. WISE and IGTF will therefore continue to be two important bodies where such issues can be worked on and agreed. Operations see the need to support multiple identity assurance levels and to better support the wider diversity of communities with which EGI engages. These also have a bearing on the trust fabric (operational distribution), as well as the policies and the coordination (better review of VO practices, continuous assessment of policy) and the impact of having to chase down incidents through VOs (increased workload on the IRTF). There have been a growing number of security incidents and vulnerabilities reported that require appropriate monitoring in place.
- **Data Protection and Privacy (GDPR).** Services and data need to be provided ensuring confidentiality, integrity and accessibility in compliance with EU regulations by defining and enforcing community-defined policies and controls. Where personal data is concerned,

controls must be introduced to comply with the upcoming European General Data Protection Regulation (GDPR) and its adaptations in the national regulations.

3.3.2 Plans to address the current open issues

The security coordination activities will continue to be funded after the project as an EGI core activity. These funding may be integrated by other external sources of funding, such as EC H2020 projects, mostly to support the evolution of policies and tools to cover new technologies and services.

This sub-section presents some of the ways in which EGI and the security team will address the operational security issues. It also describes areas of actions but this is subject to identifying and successfully securing additional funding.

The work will continue from the platform of security operations, as today, and it will also continue the process of optimization by streamlining and consolidating tasks within the general operations teams. To make this smooth the tool set will be revised, in particular for security monitoring needs, to support escalated controls: The Security Operations team can then focus on third line support, whilst allowing integrated follow-up of security and other operational issues with the resource centres.

For security monitoring, EGI will need to identify overlaps with other infrastructures and external service providers, to make sure the concepts could be applied for them too, maximising the use of the existing monitoring facilities, analysing new risks and extending the monitoring – where needed - to take these into account and detect such risks. When integration with other infrastructures is needed, security Operations will need to extend significantly the way how data from multiple sources are processed and evaluated. Security-related data requires special attention and must be processed by carefully crafted methodologies that will balance occurrences of false alarms and other irregularities. Collaboration with GÉANT, as a collaborating e-Infrastructure, may expand the dataset that can be used by the security team, with network monitoring data. Although this collaboration is in a very early stage, these inputs may be particularly relevant for the security of the federated cloud.

Training is an essential element for a secure EGI, as it helps to ensure that appropriate security expertise is available at the resource providers, NGIs and user communities. Explicit EGI-wide security challenges (such as the “SSC”s) and expert-level training have met with high approval and shown significant improvements in incident response capabilities at sites and in NGIs. Security training will ensure expert training opportunities will be available to sites, NGIs and user communities and provide coordination for continued security challenges in EGI.

EGI will need to continue working with other projects which are innovating and bringing in new technologies and paradigms. AARC and the IGTF, as well as the AAI for EGI and the user community activities are one obvious example. Collaboration with the WISE Community is supportive of this extended scope, by defining and sharing community best practices.

Since research is global, security and authentication-related policies must be coordinated with peer infrastructures in Europe and elsewhere, and we will be exposing our processes to the community as a whole, e.g., via ongoing membership of the WISE community, FIM4R and REFEDS, and leadership of appropriate working groups such as SCI. Other means may become available and will be used if appropriate.

An important thrust in the coming years will be to build trust and create effective interoperability with other e-Infrastructures that are currently still disjoint, and with our key Research Infrastructures, and, when appropriate, with dedicated security groups in Europe (TF-CSIRT, GEANT) and in the USA, for example REN-ISAC. At a small scale, EGI already collaborate with the security teams from EUDAT and PRACE and this collaboration will continue. EGI also have collaborated with XSEDE, OSG, NCSA and CTSC in the USA and will aim to build more on these connections, including collaboration with Infrastructures in Asia/Pacific.

In terms of research infrastructures, WLCG/LHC/HEP is already closely integrated and this will continue. Other Research Infrastructures, particularly those with specific security needs such as ELIXIR or BBMRI and other research infrastructures in the biological and medical sciences (such as those collaborating in CORBEL), are potential partners and closer collaboration will be investigated. Collaboration is open to all other communities, and the appropriate level of engagement will be considered as these infrastructures address security capabilities and opportunities thereby arise. EGI is explicitly open to offering security services (incident response, training, policy building) to such research communities if this is something they are interested in. Yet the security team are aware of the sensitivities in this area and will guard against 'forcing ourselves' upon them. A business model would have to be identified and implemented to provide appropriate levels of funding for such activities.

More in detail the roadmap for security operations will develop in the following four areas:

1. **Streamlining of EGI security policies, procedures and assessments**

This activity will start from the platform of security operations, as today, but continue the process of optimization by streamlining and consolidating tasks within the general operations teams wherever possible. To make this smooth the security team will need to revise the tool set, in particular for security monitoring needs, to support escalated controls. The Security Operations team can then focus on third line support, whilst allowing integrated follow-up of security and other operational issues with the EGI resource centres. The complex third-line issues are more appropriate for the realm of IRTF and other EGI security bodies (SPG and SVG). Typical tasks will be developing security policies and procedures, understanding vulnerabilities and producing the mitigation instructions (advisories), and in forensics as part of the Incident Response activity.

Security assessment became a vital service in EGI, which provides an overview about the state of security of service components in EGI. The site certification process involves security-related steps that make sure resources are in a good shape before they constitute a part of the production infrastructure. EGI Security will continue to work on the assessment of new technologies and services so that they do not expose known vulnerabilities. Extending the scope of these tools so

that they are able to cover other infrastructures and integrate other approaches in a scalable way would be desirable.

2. **Building trust and collaborating with other Infrastructures**

Given our closer collaboration with EUDAT and the prominence of data and open science clouds, doing everything to ensure that other Research Infrastructures and e-Infrastructures benefit from common shared security expertise is highly desirable.

EGI will promote interoperation and collaboration by exposing our processes to the community as a whole. In the first instance, this will be achieved via ongoing membership of the WISE community and leadership of appropriate WISE working groups. EGI contribution to WISE will continue to define 'areas of interest' where teams from different infrastructures can align and integrate in ways that suit their operational model. WISE and SCI offer a scheme for doing so, and, based on that, EGI can generate the operational implementation. Other means may become available and will be used if appropriate.

Leveraging our wide network of contacts across security in academia and research will continue to be important and the security team have much to offer and will continue to do so wherever possible for the benefit of all. Wider collaboration, both at the service (infrastructure, EGI, EUDAT) and network (GEANT, Internet2) level can help identify long-term trends in attack profiles and methodologies. Although dependent on the amount of information that can be shared, the correlation of service and network forensics data can be used to better identify ongoing attacks and apply prevention techniques for emerging risks.

3. **AAI policies and harmonisation**

The security team will continue to collaborate with the AAI policy harmonisation and community engagement activities being pursued by AARC2 and IGTF. Community and EGI Infrastructure requirements for AAI services will be provided to the Federated Identity Management for Research (FIM4R) activity in its production in the coming months of version 2 of its earlier paper in 2013 (Ref). Template policies produced by the AARC2 project will be adopted and deployed on the EGI Infrastructure and the security team will provide feedback and requirements for changes or additions as necessary.

The EGI Security Policy Group will run the process for assessing the combined adequacy of AAI assurance levels as requested by Communities proposing to use authentication credentials base on the IGTF Dogwood assurance level to ensure that their own procedures meet the necessary standards.

4. **Data protection, privacy and the GDPR**

In view of the rapid integration of data clouds and data in the European Open Science cloud, Data Protection and Privacy is an important topic for the Infrastructures and also for some research communities (e.g. in biological and medical research). The security team will continue to address issues of policy and operational procedures related to this.

Where personal data is concerned, controls must be introduced to comply with the upcoming European General Data Protection Regulation (GDPR) and its adaptations in the national regulations. EGI will work closely with others, including GEANT and AARC2, in the Research and Education arena that are actively working on codes of conduct, policies and best practices to meet the requirements of the GDPR.

The Security Policy Group will revise the existing EGI policy framework on the Processing of Personal Data, as required to address the GDPR and any agreed new Codes of Conduct, as expected from the work by GEANT and AARC2. Templates will be produced for Data Privacy statements by all EGI and Community services, consistent with the EGI framework. The most important milestone in this activity will be to have data privacy statement consistently published by all the EGI service providers.

The increase in scope, number of parties covered, and much broader range of services and organisations will push the boundaries of the effort available to the EGI-CSIRT as planned in the future core activities. The actions and tasks will have to be properly prioritized, and planned in scope to fit with the available manpower. Involving the service providers and other external organisations in the process will be critical, as the current collaborative model, organisational structure, and engagement methodology of EGI-CSIRT shown to be are effective and appreciated by the global community in both Research and e-Infrastructures and private sector. EGI CSIRT model may grow in scope, impact, and visibility, and thereby bring concrete benefits to Research and e-Infrastructures that decide to collaborate with EGI.

4. Software and service validation

4.1 UMD and CMD

Unified Middleware Distribution (UMD) is the integrated set of software components contributed by Technology Providers and packaged for deployment in EGI after being validated as production-quality.

UMD4 is the current supported UMD distribution. It supports the following Linux distributions: CentOS7, SL6 and Ubuntu 16 (Xenial). UMD3 will still receive security or critical updates for SL6. UMD3/SL5 and UMD3/Debian are not supported anymore.

The yaim component, a common configuration management script used my many HTC middleware components, is not supported anymore for the UMD4 software. Yaim has been replaced by component-specific documented procedure to install, configure, and test the product. Examples of alternative configuration tools are Puppet recipes, Ansible recipes, or custom scripts and step-by-step guides mainly for products with simple configuration. Puppet recipes are currently the most popular standardized configuration mechanism provided by the product teams.

UMD4/SL6 started as a mirror of UMD3/SL6, without the products that were about to reach or have already reached end of life. Products based on SL6 are now distributed through UMD4/SL6, and only security updates are distributed through UMD3/SL6.

The Cloud Middleware Distribution (CMD) aims at distributing OpenStack and OpenNebula integration components (not the cloud management systems themselves) that are products that are deployed on top of OpenStack/OpenNebula mainstream distributions, other products that enable the IaaS federation, even if they're not directly dependent on OpenStack/OpenNebula. The main reason to release separate distributions from UMD is that the release cycle of OpenStack and OpenNebula is different from the UMD one; hence basically whatever depends on it is moved to a different dedicated distribution. The client components will be distributed through UMD.

In summary, CMD is actually organized in two different distributions:

- CMD-OS (OpenStack)
- CMD-ONE (OpenNebula)

and components are released as follows:

- OpenStack specific components, in CMD-OS
- OpenNebula specific components, in CMD-ONE
- common cloud components (information provider, accounting, appliance synchronization management), in both CMD-OS and CMD-ONE

Every CMD major release is associated to a specific OpenStack release or OpenNebula release and follows the respective release cycles. The first version of CMD-OS supports OpenStack Mitaka, the first version of CMD-ONE (to be released) supports OpenNebula 5.

All the products in CMD must be available both as CentOS7 and Ubuntu Xenial packages.

The software distributed in UMD and CMD goes through the Software Provisioning process, which goal is to validate the software to be production-ready, and to reduce as much as possible the probability that the new released deployed in production cause problems to the services. The UMD Software Provisioning process can be summarized by the following steps:

1. Technology Providers submit new software releases to the EGI software provisioning process
2. Software Assessment through Quality Assurance and Staged Rollout
3. Provide early feedback to the developers about outcome of the software provisioning process
4. Release in UMD and CMD the products that successfully completed the validation steps, to be deployed in production services

In particular, the Software Assessment step is done in two phases:

1. Quality Assurance, consisting in the software to be installed and configured by the UMD team using the documentation and procedures provided by the software development team; if everything is OK, the software goes through the next step, called
2. Stage Rollout, consisting in testing the software on a given Resource Centre interested in trying the software in advance, and so acting as Early Adopter.

The Fedcloud components developed in JRA2 are already being released to the CMD, currently there is no full coverage by CMD, but this is going to be achieved by the end of the project.

4.2 Containers

At the moment UMD and CMD are releasing in repositories supporting *rep* and *deb* package management systems, these being the most common and popular both among the developers and the resource centers. In parallel to the traditional packages management systems, containers installations are increasing in popularity among the technology providers, in particular the INDIGO Datacloud[16] project that is delivering components for the federated cloud portfolio. Docker containers have several advantages for both developers and system administrators, and they are expected to increase in demand in the future.

[16] https://www.indigo-datacloud.eu/

The containers are already used in the FedCloud, the federation layer software is available as containers to be deployed inside a dedicated virtual machine, which images is made available by the EGI cloud team.

To support containers EGI will have to apply a Software Provisioning process similar to what is implemented for the packages, subject to the same requirements.

The Technology Provider must provide the same (or equivalent) information. Which include: for the development team: TP leader and contacts; and for the releases provided through containers: documentation, release notes, verification procedure, helpdesk support unit and QoS level, support calendar.

The Verification procedure will consist in successfully starting and running the container on the supported Operating Systems (for example CentOS7 and Xenial), to demonstrate compatibility with a set of hosting solutions.

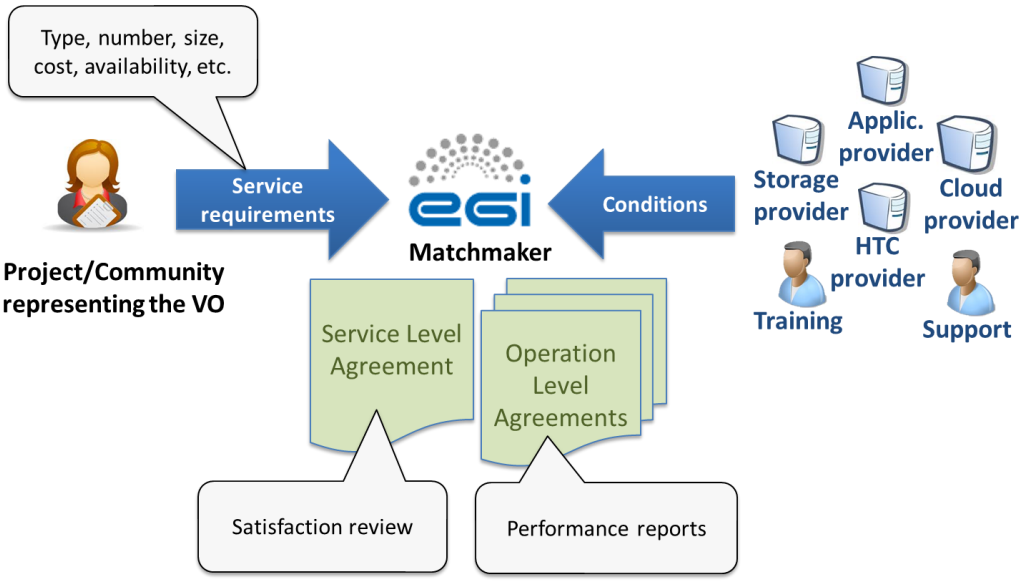
The Staged Rollout report of the software released in the container must be available, but it can be provided by an early adopter deploying the same software using packages, if the same software release has been submitted, for example, to UMD both with containers and rpms.

The successfully validated containers will be then made available in a dedicated DockerHub repository managed by EGI, and containing only validated containers. Ideally the EGI resource providers should use only this repository to download docker images.

5. Service provisioning

5.1 SLA and OLA framework evolution

To facilitate the allocation of resources to fulfil the needs of a specific group of researchers and allow them to better plan a research programme, EGI has implemented the framework depicted in the following figure:



The process starts by collecting the technical requirements, expressed in terms of number of CPU cores, disk space, software packages, and more, from the customer to support their specific research activity. EGI uses customer's requirements to collect offers from the different providers of the federation that can fulfil the use case. EGI acts as matchmaker establishing several Operational Level Agreements (OLAs) with the providers supporting the use case, and a single Service Level Agreement (SLA) with the Customer, acting in this way as a central contact point between customers and providers.

EGI coordinates and monitors the service delivery in order to measure the fulfilment of the agreed service level targets, taking actions in case of deviations, and manages the Customer complaints and disputes. This monitoring is technically implemented by checking that the monthly services availability performances meet the service targets. The performance report, describing how the service is delivered, is sent to the Customer every 6 months. Every three, six months EGI runs Customer Satisfaction Review process to review the whole agreement and identify possible improvements for the SLA and services. For what concern the Customer's responsibility they have

to acknowledge EGI and the providers in the scientific publications benefiting from the service offered.

The benefit of the SLA framework can be summarised as follows:

- For the research communities:
  - Better communication and clarity on expectations;
  - Increased confidence that services will be delivered;
  - Easier future planning of research activities.
- For the resource providers:
  - Direct communication with user communities and clarity on expectations ;
  - Clear responsibilities and rules/policies concerning usage of the resources;
  - Recognition and greater visibility to role of the provider by requiring an explicit acknowledgment.
- For EGI Foundation:
  - Promoting the EGI service value with funding agencies and policy makers at national and European level;
  - Being seen as mature partner;
  - Ensuring a foundation of a control process to what is being delivered in the EGI Federation.

For the resource centres or communities not included in dedicated VO SLAs, the Corporate Level Service Level Agreement[17] is applicable for all services provided to support business processes according to the current valid EGI service catalogue.

As a result of resource allocation process 37 providers from 15 countries have allocated: 152M computing hours for HTC, 169 TB of storage, 4.9 TB of RAM and 1410 vCPU cores.

[17] https://documents.egi.eu/public/RetrieveFile?docid=2733

Customer	Start	End	Service Type	Providers	Resources Allocated
BioISI	Aug. 2016	Jan. 2018	Cloud Compute		84 vCPU cores, up to 1TB of RAM and 20 TB of storage
NBIS/BILS	Dec. 2015	Dec. 2017	Cloud Compute		172 vCPU cores, 400GB of RAM, more than 7TB of block storage and 2 TB of object storage
DARIAH	Apr. 2016	Sept. 2017	Cloud Compute		30 vCPU cores, 70GB of RAM and 2TB of object storage
DRIHM	Jan. 2016	Jan. 2018	High-Througput		57.51 M HEPSPEC, 374 GB of RAM and 13.5 TB of storage
D4Science	Sept. 2016	Dec. 2017	Cloud Compute		210 vCPU cores, 584 GB of RAM and 12.5TB of storage
EMSODEV	Sept. 2016	Dec. 2017	Cloud Compute		340 vCPU cores and 9TB of storage

EXTraS	May 2016	Jan 2018	Cloud Compute		60 vCPU cores, 240 GB of RAM and more than 1.6TB of storage
LSGC	May 2016	Jan. 2018	High-Throughput, Cloud Compute		148 vCPU cores, 296GB of RAM and 2.5TB of storage 44.6M HEPSPEC and 25.85TB of storage
MoBrain	Jan. 2016	Jan. 2018	High-Throughput, Cloud Compute		60 vCPU cores, 360 GB of RAM and 2TB of storage 60M HEPSPEC, 26GB of RAM and more than 59RB of storage
Peachnote	Apr 2016	Sept. 2017	Cloud Compute, Online Storage		104 vCPU cores, 162GB of RAM and 8TB of storage
Terradue	Jan. 2016	Jan. 2018	Cloud Compute		538 vCPU cores, 1.4TB of RAM and 10TB of strorage

Table 9: VO SLAs active, July 2017

The list of active VO SLAs is reported in Table 9, the disciplines of the supported communities are diverse, including for example humanities, earth observation, agriculture, and structural biology.

The process to define and then manage SLA at the moment is entirely manual. During the project the workflow has been designed and implemented, producing good initial results, for the future it will be supported by technical tools as well.

The workflow and the activities described earlier in this section can be summarized as: negotiation of SLA/OLA including selecting the resource providers, and monitoring the status of the SLA and the quality of the services provided. The experience gained during EGI-Engage suggests focusing the automation developments in the second part of the workflow, since the negotiation requires human interaction to properly define the user requirements and motivate the resource providers to contribute to the use cases.

To implement any automation in the process of monitoring the service provisioning after the VO SLA agreement there is need to programmatically obtain the providers and the services contributing to a specific SLA, for example to produce automated monitoring reports. This

development will make possible also automatic reporting to the customer and the provisioning of dashboard and dedicated views in the operations tools, if necessary.

This development and other improvements will be covered in future development activities supported by EGI Foundation or future projects.

5.2 Addressing the long tail of science

The Long Tail of Science pilot has been implemented as part of the SA1 activity in EGI-Engage project. The overall goal of this pilot was to provide simplified access procedures to individual users or small groups of researchers who need to access e-Infrastructures for supporting their day-by-day working activities.

The main outcome of this pilot is the creation of the Applications on Demand (AoD) service[18] for supporting research activities. The service was specifically designed for individual researchers, small research teams and early-stage research infrastructures that do not have dedicated computational and storage resources, online applications and science gateways to perform scientific data analysis. The service, available as a beta product, is available at http://access.egi.eu and, through a lightweight registration and user identity vetting process, allows user-friendly access to a growing number of applications and applications hosting frameworks (Science Gateways, Virtual Research Environments) that are configured to use the dedicated pool of cloud computing and HTC clusters from EGI. The service operates as an open and extensible 'hub' for providers and e-infrastructure user support teams who wish to federated and share applications and services with individual researchers, or small, fragmented communities, typically referred to as 'the long tail of science'.

Scientific applications already available for access are the following:

- Application and data analysis frameworks: Jupyter Notebook, Docker, Apache Tomcat, Hadoop, Marathon, and Chronos.
- Life sciences: Galaxy, ClustalW2, Chipster, NAMD and AutoDock Vina.
- Data analysis: GnuPlot, Octave and the Statistical R for Computing.
- Humanities: the parallel Semantic Search Engine.

Application development and hosting environments available for access:

- Catania Science Gateway (CSG)[7]
- WS-PGRADE Portal[19]
- Elastic Cloud Computing Cluster (EC3)[20]

[18] http://csgf.egi.eu/c/portal/login?openIdLogin=true
[19] https://ltos-gateway.lpds.sztaki.hu/c/portal/login?openIdLogin=true

- The EGI VMOps dashboard[21]

The service is currently supported by several cloud providers of the EGI Federation: BIFI and CESGA (Spain), CYFRONET-LCG2 (Poland), INFN-BARI and INFN-BARI (Italy) and BEgrid-ULB-VUB (Belgium).

On June 13th 2017, EGI organized a webinar[22]to officially introduce and provide a high-level overview of the EGI Applications on Demand (AoD) service. The target audience of the webinar were:

- **NGIs and National User Support Teams**: They can use the service to serve national users, or they can use this European service to promote and make available their national applications and gateways/VREs to foreign users.
- **Representatives of research infrastructures or scientific communities/projects**: They can use the service to serve their long-tail users with generic or domain specific applications, before/without committing to long-term resource allocation through EGI.
- **Researchers and small research teams**: They can learn about the applications and tools that are available for them in this service.

After the webinar, EGI published the new service in its Services Catalogue[23] and has started to promote its adoption in different NGIs. As result of this promotion, we have collected expressions of interests from some NGIs (e.g.: NGI_Armenia, NGI_RO, NGI_HR and NGI_IT) who are planning and/or evaluating the possibility to adopt the service to target the requirements of their national research communities.

EGI is investigating the possibility to extend the solutions offered to the end users, configuring some thematic and general-purpose services such as Jupyter and Galaxy as a service.

[20] https://servproject.i3m.upv.es/ec3-ltos/index.php
[21] https://dashboard.appdb.egi.eu/vmops

[22] https://indico.egi.eu/indico/event/3378/
[23] https://www.egi.eu/services/applications-on-demand/

6. Conclusions

EGI-Engage project produced many results on new services, platforms and solutions that can be provided by the resource centres of EGI to the communities.

The competence centres have integrated community specific services with the EGI infrastructure. The marketplace will allow advertising external service providers for the EGI users. These new use cases expand the area of competence of the EGI operations beyond the federated resource centres, and will require designing new processes and policies to ensure a minimum level of compatibility with these external services. This new processes will be designed during the end of 2017; and they will be implemented during the first half of 2018 or as soon as new use cases approach.

The new communities are focusing on cloud IaaS and higher level services, such as PaaS, SaaS and managed services. IaaS operational requirements have been addressed during the project, and the evolution of the operations tools, policies and procedures must continue to further expand the service catalogue of EGI, maintaining the infrastructure to be secure and reliable. The security policies and processes will evolve to address the new technologies and usage scenarios requirements, the other operational tools and procedures will be updated as well. One example is the certification procedure of a resource centre, new service types may require some specific steps to be performed to certify a resource centre providing such services. This is a continued activity, which will very likely increase the speed during 2018, when new projects will bring more services, and more service providers, to integrate.

Central Operations will also focus on reducing the effort required to run an operations centre, and resource centre, to mitigate the uncertainty in effort availability in some operations centres. A first approach is to reduce the number of services that are deployed at national, or EIRO, level, possibly replacing them with central instances. This will happen with WMS, for example, during 2018.

The e-Infrastructures ecosystem is expanding and the number of communities with use cases that cross the borders of a single federation will likely grow. Therefore strengthening the collaboration with the other European and international infrastructures is among the future priorities as well. This will be achieved on thematic working group, such as WISE, or in the context of existing and future projects, for example AARC2 and EOSC-Hub. AARC2 has already started, and also the WISE community is already active, the future EOSC-Hub project, starting in 2018, will strengthen the collaboration with EUDAT starting in 2018.

All these activities have been, at different levels, initiated during the EGI-Engage project, and there are already solid bases to continue the work beyond the end of the project.