D5.5 Second report on maintenance and integration of federation and collaboration services

Lead Partner:	KIT
Version:	1
Status:	Under EC review
Dissemination Level:	Public
Document Link:	https://documents.egi.eu/document/3645

Deliverable Abstract
The document outlines the second report on maintenance and integration of federation, access enabling and collaboration services, one of the key components of the EOSC Federating Core, a fundamental asset that EOSC-hub provides to EOSC. It provides a technical description of enhancements for the EOSC-Hub services in Work Package 5 (WP5), results of integration activities and collaboration work with other initiatives made during the second year of the project. The report identifies the integration gaps and elaborates the future plans for WP5 services.

COPYRIGHT NOTICE

DELIVERY SLIP

Date	Name	Partner/Activity	Date
From:	Nicolas Liampotis	GRNET	20/07/2020
	Kostas Koumantaros	GRNET	
	Themis Zamani	GRNET	
	Roksana Rozanska	CYFRONET	
	Cyril L'orphelin	IN2P3	
	Pavel Weber	KIT	
	Marcus Hardt	KIT	
	Alexandros Nakos	IASA	
	Ivan Diaz Alvarez	CESGA	
	Jens Jensen	STFC	
	Greg Corbett	STFC	
	Raphael Ritz	MPG	
	Daniel Kouril	CESNET	
	Christos Kanellopoulos	GEANT	
	Sander Apweiler	Julich	
	Mischa Sallé	Nikhef	
	Slavik Licehammer	CESNET	
	Enrico Vianello	INFN	
Moderated by:	Malgorzata Krakowian	WP1/EGI.eu	
Reviewed by:	John Alan Kennedy	MPG/WP6	
	Joao Antonio Tomasio Pina	LIP/WP4	
Approved by:	AMB		

DOCUMENT LOG

Issue	Date	Comment	Author
v.0.1	22..01.2020	Table of Content ready	Pavel Weber
v.0.2	2.02.2020	The first draft with all sections ready	
v.03	20.04.2020	All contributions are provided	WP5 service/tool owners
v.0.4	25.06.2020	Added executive summary	Pavel Weber
v.0.5	05.06.2020	Ready for review	Pavel Weber
v.0.6	15.06.2020	Review	
v.1.0	20.07.2020	Corrections from review are implemented	Pavel Weber

TERMINOLOGY

https://wiki.eosc-hub.eu/display/EOSC/EOSC-hub+Glossary

Terminology/Acronym	Definition
AAI	Authorization and Authentication Infrastructure
AARC	Authentication and Authorisation for Research and Collaboration
AC	Attribute Certificate
AppDB	Applications Database
AppDB IS	AppDB Information Service
AppDB VMOps	AppDB VM Operations
AUP	Acceptable Use Policies
BDII	Berkeley Database Information Index
CA	Certification Authority
CDI	Collaborative Data Infrastructure
CMDB	Configuration Management Database
DPMT	Data Project Management Tool
EGI	European Grid Infrastructure
EOSC	European Open Science Cloud
EUDAT	European Data Infrastructure
GDPR	EU General Data Protection Regulation
GGUS	Global Grid User Support
GOCDB	Grid Operations Configuration Management Database
HA	High Availability
IAM	Identity and Access Management System
IdP	Identity Provider
IGTF	Interoperable Global Trust Federation
LB	Load Balancing
LoA	Level of Assurance
OIDC	OpenID Connect
OLA	Operational Level Agreement
PKIX	Public-Key Infrastructure (X.509)
SDT	Service Description Template
SLA	Service Level Agreement
StaR	Storage Accounting Record
SOCRM	Service Order and Customer Relationship Management
PID	Persistent Identifier

SP	Service Provider
SMS	Service Management System
SAML	Security Assertion Markup Language
TRL	Technology Readiness Level
VM	Virtual Machine
VO	Virtual Organisation
VOMS	Virtual Organization Membership Service

Contents

Executive summary

The activities in work package 5 started according to the initial plans reported in deliverable 5.1 underwent multiple adjustments to meet the changing requirements provided by other governance and technical work packages in the project, agreed collaboration work with other projects, as well as research communities and other stakeholders to federation services, which are being constantly collected and analysed in WP5.

The federation services in WP5 are the EOSC core services, which guarantee the distributed operation of the EOSC Hub and integration of generic, thematic services, as well as support for a federated Service Management System in the EOSC ecosystem. They also offer a set of capabilities for any new onboarded service like service discovery and ordering, access, monitoring, accounting, helpdesk etc. for the benefit of Service Providers of onboarded services. The federation and collaboration services are the components of the EOSC-hub Key Exploitable Results (KER) "Internal Services Provided in the Hub Portfolio" and "EOSC Portal and Marketplace".

The initial WP5 roadmap, development and integration work of federation services have been significantly modified to meet the requirements towards integration with EOSC Portal in the scope of cross-project EOSC Portal Collaboration Agreement between EOSC-hub, OpenAIRE-Advance and eInfraCentral projects. This integration work has been conducted for the major federation services in WP5.

The EOSC Portal is integrated with EOSC Portal AAI, which is a part of the infrastructure layer of the EOSC-hub AAI. It is connected to multiple Community AAIs to allow researchers to access the underlying services and resources using their community identity, including their roles and other authorisation-related information managed by the community.

The integration activities of the Marketplace with the EOSC Portal were focused on definition and further development of a single Service Database and the appropriate data APIs in which the service descriptions are maintained through the Marketplace as well as further development of automatic order propagation to service providers and flexible order management. Each stage of the order execution (New, assigned, implementation, Ready etc.) is reported back to the customer and can be seen in the EOSC Portal.

The integration of the Helpdesk with the EOSC Portal provides the unique point of access for users and customers of EOSC to submit incidents, make service requests from the portal allowing professional management of all the customer requests.

The ARGO monitoring system has implemented a pilot integration with the EOSC portal using the topology it delivers to monitor all services listed and to provide a view of their status. The main goal is to check the validity of the services onboarded in the portal and to identify faulty ones.

Apart from the highlights on integration work with EOSC Portal described above, the federation services have undergone many enhancements according to the roadmap provided in the previous deliverables. A few major achievements in the second year with outlook will be provided in the summary of this deliverable.

1   Introduction

The document provides a summary of maintenance activities, enhancements and integration results for EOSC Hub federation and collaborative services for the second reporting period for work package 5 of the EOSC-hub project. The deliverable provides a more detailed description of the development and integration work on the second release of the core services of the EOSC Hub, reported in deliverable 5.4 accomplished with the analysis of the achievements for major federation services, identification of integration gaps and proposed solutions.

Having lots of technical details, the deliverable aims at providing general directions of the development and integration of EOSC core services and major distributed systems like EOSC Hub AAI or EOSC Hub monitoring.

The content of the document is divided into chapters which reflect the main tasks in WP5. Trying to avoid repetition of the description of services and their components, we provide a reference to the D5.1, which contains a detailed initial description of the high-level architecture in each section for a dedicated service, followed by a summary of the major service enhancements and integration results achieved during the reporting period. At the end of the document, a short summary with outlook is provided followed by the current roadmap for all federation services in the package.

2 Identification, Authentication, Authorisation and Attribute Management

2.1 Overview

The EOSC-hub AAI enables seamless access to research data and services in EOSC-hub in a secure and user-friendly way. It comprises different AAI services, namely B2ACCESS, Check-in, eduTEAMS and INDIGO-IAM, all with a Technology Readiness Level above TRL 7. These AAI services are connected to eduGAIN as service providers and, at the same time, act as identity providers from the services point of view, in order to allow users to use their credentials from their home organisations for accessing EOSC-hub resources. The suite of EOSC-hub AAI services also includes Perun, an Identity and Access Management system, which can be used by Check-in and eduTEAMS for managing users within organisations and projects, as well as managing access rights to the services. There are also Token Translation Services such as WaTTS and MasterPortal, which provide mechanisms that enable translation between different protocols or technologies. The RCauth.eu service, in particular, is an Online CA that can identify entities on-the-fly based on federated credentials and issue to them X.509 credentials in real-time, focussing on conversion from SAML to X.509 standard.

The EOSC-hub AAI follows the architectural and policy recommendations defined in the AARC project [R1], which builds on existing best practices in the scientific community and provides clear guidance for implementing access management for international research collaborations. The EOSC-hub AAI provides the following features:

- Support for different authentications providers, including:
    - Institutions from national identity federations in eduGAIN.
    - Social media (e.g. Google, Facebook, LinkedIn).
    - Other external authentication providers such as ORCID, GitHub or community-operated identity providers.
- Access to resources using different login credentials (e.g. institutional and social) via identity linking.
- Access to multiple heterogeneous (web and non-web) services and resources using different technologies. Non-web-browser based use cases include APIs and command line access (e.g. via SSH or OAuth2).
- Aggregation and harmonisation of authorisation information (e.g. groups and/or roles) from multiple sources.
- Adoption of standards and open technologies, including SAML 2.0, OpenID Connect, OAuth 2.0 and X.509v3 to facilitate interoperability and integration with the existing AAIs of e-Infrastructures and research communities.
- Adoption of policies compliant with global frameworks (e.g. REFEDS Research and Scholarship entity category [R2] and Sirtfi [R3]) in order to:
    - Support services in receiving and processing consistent user attributes in compliance with the minimal disclosure principle.

○ Ensure good practices in operational security.
○ Enable the coordination of incident response across federated organisations.
● Expressing different levels of trust in the user identity assertions using standard frameworks such as the REFEDS Assurance Framework [R4].

A high-level view of the EOSC Hub AAI is provided in Figure 2-1. Following the AARC-BPA-2019 [R51], we distinguish between two types of AAI services:

● **Community AAI service:** enables the use and management of community identities for access to resources
● **Research/e-Infrastructure Proxy service:** enables access to resources offered by Service Providers connected to a research infrastructure or e-Infrastructure
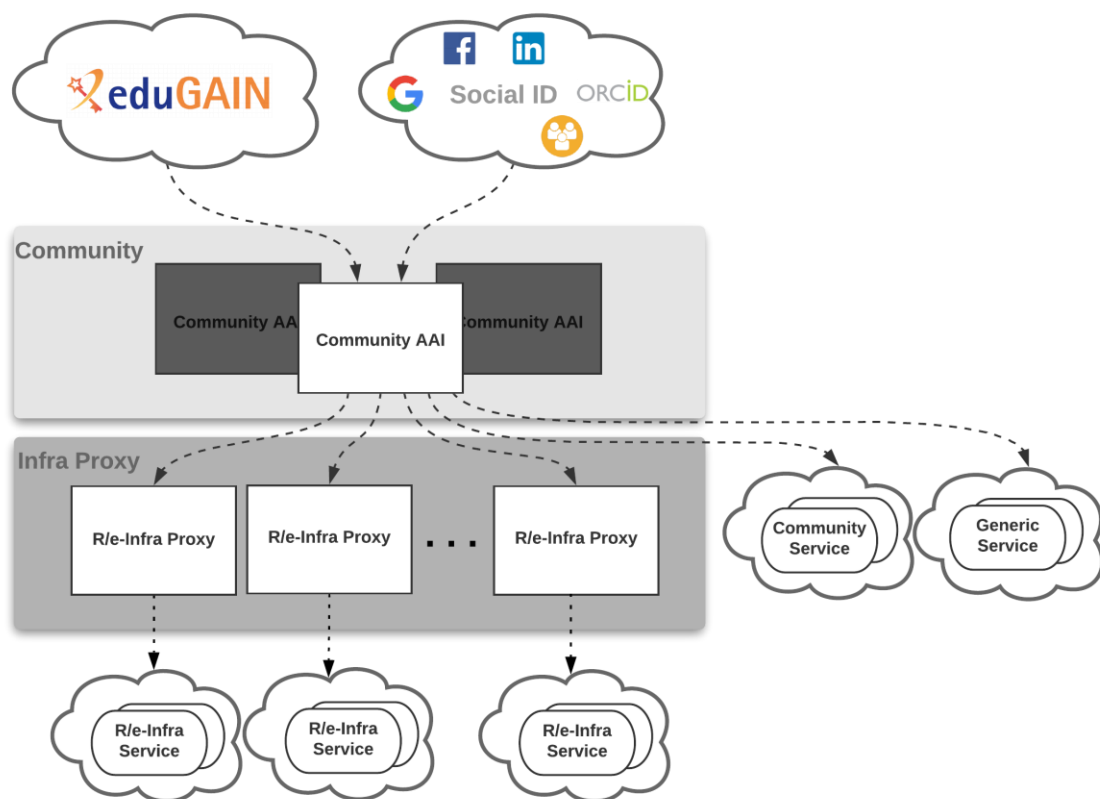
Fig.2-1 - High-level view of EOSC-hub AAI architecture

The Community AAI services act as the interface between individual researchers and resources. A community in this context means a group of users, of any size and of any duration, organised with a common purpose, and jointly granted access to resources. Trust is an emergent property of communities. Trust in this sense means a community's ability to know and determine its users and their permissions. The EOSC-hub AAI builds on the trust that exists within well-managed scientific communities and instead of trying to grow any one of those to a global context, it establishes a framework within which many such communities can co-exist and access resources.

The Research/e-Infrastructure Proxy services use similar components and technologies as the Community AAI. However, the Research/e-Infrastructure Proxy performs a very different role, as it is tasked to provide access to resources made available by an Infrastructure. The Infrastructure Proxy, enables Infrastructures with a large number of resources, to provide them through a single integration point, where the Infrastructure can maintain centrally all the relevant policies and business logic for making available these resources to multiple communities.

The EOSC-hub AAI provides an initial implementation of the EOSC AAI including a set of interoperability guidelines. These guidelines along with an implementation roadmap and a set of identified challenges are maintained in the project wiki [R5].

2.2 B2ACCESS

A detailed description of the B2ACCESS service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

2.2.1 Maintenance activities

In the reporting period we updated the underlying software unity to version 2.8.2. And kept other used packages up to date. During the unity update a short downtime (a few minutes) was needed to switch to the new release and update the internal database. The virtualisation layer for the server was also updated which required a reboot of the server and included a downtime of a few seconds. Besides these two planned and announced downtimes, no further downtimes were required. Furthermore, the integration with eduGAIN was updated to the new certificate infrastructure of the DFN which provides the current access to eduGAIN.

2.2.2 Summary of service enhancements

In the last year several small enhancements for the users have been made. Email addresses from users who authenticated with EGI Check-in do not need to be confirmed anymore, because Check-in does already validate the email addresses of the users. eduTEAMS has been added as an additional identity provider so that users with an account in eduTEAMS can use services, connected to B2ACCESS, too. With the update to the newer unity version an additional group management endpoint has been enabled. Using this endpoint the group management can be done from the group itself by a special group administrator. In the past the group management was done by the administrators of the service, who were contacted by the group administrator. The discovery service was updated with the update of unity and provides a modern look to the identity provider selection. Further B2ACCESS remembers the last used identity provider of the users and offers it directly at the next login, which simplifies and speeds up the next login.

2.2.3 Future plans

Within the next year we plan to simplify the access for users with accounts from Check-in and eduTEAMS by harmonizing the use policies. With harmonized use policies, the users do not need to accept the policies of the other infrastructures and can access the services directly. Furthermore, the underlying software stack will be updated.

2.3 Check-in

A detailed description of the Check-in service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

2.3.1 Maintenance activities

The production operation of the EGI Check-in service involved technological upgrades of the underlying framework and libraries in order to take advantage of new features and robustness, as well as continuous optimisation of the architecture and automation of new tasks to ensure the uninterruptible and performant operation.

2.3.2 Summary of service enhancements

2.3.2.1 Enhancements to identity provider interface

- Added support for additional authentication providers:
  - GitHub
  - Bitbucket

2.3.2.2 Enhancements to service provider interface

- Added support for the OAuth 2.0 device authorization grant [R8]. This OAuth 2.0 extension enables devices with no browser or limited input capability to obtain an access token.
- Added support for expressing resource capabilities according to AARC-G027 [R9]. Capabilities define the resources or child-resources (e.g. RCauth Online CA, GOCDB) a user is allowed to access.
- For services that rely on X.509 certificate-based access, Check-in added the ability to provision the user's identity attributes, including VO/group information as VOMS proxy certificates.

2.3.2.3 Enhancements to User Enrolment and Group/VO Management

- For users without a personal certificate, Check-in added support for linking a certificate issued by the RCauth Online CA to their Check-in profile.
- Added support for parsing full name information received by the user's home organisation identity provider to extract the user's given name and surname attributes.
- Improved integration with Perun to support retrieving VO & group membership information for users registered in Perun-managed VOs/groups via Check-in. Prior to this enhancement, Check-in was only able to retrieve membership information for users registered in Perun with a personal certificate.
- Added support for storing the Authenticating Authority during user registration. The Authenticating Authority is displayed in the profile of the user under their linked organisational identities panel.
- Improved the user registration flow. Specifically, after successful registration, the users are redirected to the service they were originally trying to access.

2.3.2.4 *User interface improvements*

- Applied the EGI theme to Comanage Registry to provide a uniform look and feel across all Check-in service component UIs.
- Added paging/search functionality to allow users to filter/sort:
  - Groups, based on "Name" and "Description".
  - Group Membership, based on "Given Name", "Family Name", "Email", "Identifier" and Alphabetically.
  - Enrollment flows, based on "Name".
- Added option to make private Enrollment Flows, if the option is enabled then the enrollment flow will not be displayed in the user's profile management page under the "People->Enroll" drop down menu.

2.3.3 Future plans

2.3.3.1 *Improve integration with Community AAIs*

This enhancement will improve the user experience when users authenticate with their Community AAI (such as B2ACCESS, INDIGO IAM or eduTEAMS) to access services protected by Check-in. Improvements include:

- Skipping verification of email address when users authenticate with a verified email address [Q2 2020]
- Simplifying IdP Discovery for end-users accessing services that support the AARC IdP-hinting specification AARC-G049 [R10] [Q4 2020]

2.3.3.2 *Proxy certificate retrieval through SSH key information managed in COmanage Registry*

Users can use SSH key authentication in order to retrieve proxy certificates from the MasterPortal (see Section 2.8). Currently, this requires users to upload the ssh public key via a dedicated self-service portal [R11]. This activity will enable proxy certificate retrieval from the MasterPortal using the SSH keys uploaded by users through the COmanage Registry user profile management page [R12]. It should be noted that the MasterPortal will take into account the SSH keys from both the existing dedicated portal and the COmanage Registry. Expected time of implementation: [Q3 2020]

2.3.3.3 *OAuth2 scope-based active attribute value selection*

This enhancement will allow selecting the values of specific claims returned in access tokens and results from requests to the *UserInfo* and the *Introspection* endpoint. Value selection will be triggered by requesting scopes in the following form:

<scope_name>[:<scope_value>]

For instance, when requesting "eduperson_entitlement:<value1> eduperson_entitlement:<value2>", the eduperson_entitlement claim will only include <value1> and <value2> (assuming these values are included in the user's entitlements). Expected time of implementation: [Q2 2020]

2.3.3.4   *Improve identity linking user experience and interface*

Identity linking (also known as account linking) refers to the process of connecting the user's identity generated by Check-in with their external identities, i.e. identities created and assigned by institutional or social media IdPs. The identity linking process allows the user to access resources with a unique identity regardless of their external identity, used for authentication. Check-in currently supports *explicit* linking, which enables users to request that an additional identity be linked to their existing Check-in identity. This enhancement includes the following activities:

- The linked identities panel shown in the Check-in user management profile page will be improved by including the friendly name & logo of the user's linked identity providers.
- Check-in will add support for *implicit* linking, which will be triggered when one attribute, or a combination of attributes, of one identity correlates to one or more attributes of another identity that is already associated with a registered user. Implicit linking can prevent an individual from accidentally registering distinct Check-in identities. The identity linking considers a proper combination of assurance information, so even if the user's identities have been linked (either explicitly or implicitly), the assurance is determined based on the identity the user is authenticating with (effective identity). This is based on guidelines document AARC-G031 [R52]

Expected time of implementation: [Q3 2020]

2.4   eduTEAMS

A description of the eduTEAMS service is given in D5.3 [R13]. The release notes for the reporting period are provided in D5.4 [R4].

2.4.1   Maintenance activities

In the reporting period, eduTEAMS transitioned to the GÉANT Framework Agreement for the Amazon Web Services [R14]. The GÉANT Framework agreement, ensures compliance with EU data security and privacy regulations, enables us to use a direct connection from the AWS data network through NREN and GEANT high performance network peering arrangements and provides us with access to a global Infrastructure of 53 Availability Zones within 18 Geographic Regions.

The eduTEAMS software stack follows the semantic versioning scheme [R15]. In the reporting period, the eduTEAMS software stack had **732 changes merged**, which were incorporated into **2 major releases**, **6 minor releases** and **4 patch releases**. At the end of the reporting period the latest version was v3.0.3. These version upgrades were applied to the eduTEAMS deployments [R16], including the eduTEAMS Shared Service and all the eduTEAMS Dedicated and Bespoke deployments.

2.4.2   Summary of service enhancements

- **Improved service scalability, availability and performance.** The main focus during the reporting period has been on service scalability, stability and performance, as we had witnessed a significant uptake of eduTEAMS by research infrastructures and communities of various sizes.

In terms of improving the service availability, in the reporting period, eduTEAMS fully adopted the infrastructure-as-software approach and introduced support for zero downtime deployments regardless if it is a simple configuration, a patch, minor or major upgrade.

In terms of scalability, v3 introduced full automation for all stages of the service lifecycle, from the initialization of the infrastructure, up to infrastructure upgrades, services updates and reconfigurations.

In terms of performance, eduTEAMS now supports HTTP/2, which means that several HTTP requests can be sent in rapid succession on the same TCP connection to the eduTEAMS Service, and responses can be received out of order - eliminating the need for multiple connections between the clients and eduTEAMS.

- **Enhanced capabilities for eduTEAMS Dedicated and Bespoke.** eduTEAMS can now be deployed as a Community AAI, an Infrastructure Proxy and a combination of a Community and Infrastructure Proxy, providing a full implementation of the AARC Blueprint Architecture 2019.

- **Improved the Service Provider Registration process.** The eduTEAMS Service is now available in the eduGAIN Metadata Feed also as an Identity Provider and publishes the support for Sirtfi and GEANT Code of Conduct for both its SP and IdP interface. This allows for easier integration with Infrastructure Proxies and other SAML Service Providers which already consume the eduGAIN Metadata.

- **Extended the support for external Identity Providers**. GÉANT has joined ORCID as a member and now eduTEAMS can use the enhanced members API [R17], added support for Bitbucket and improved support for LinkedIn as an authentication source.

- **UI Improvements.** The UI of all the user facing components has been redesigned in order to improvise the usability of the eduTEAMS Service and the overall user experience.

- **AARC Interoperability Guidelines.** Improved support for **AARC-G002** "Guidelines on expressing group membership and role information", **AARC-G025** "Guidelines for expressing affiliation information", **AARC-G027** "Specification for expressing resource capabilities" and **AARC-G045** "AARC Blueprint Architecture 2019"

2.4.3   Future plans

The following plans are listed in the service roadmap for the next reporting period:

- Include Monitoring and Alerting as a Service option to the eduTEAMS Dedicated and Bespoke offering [Q2 2020]
- New improved Discovery Service [Q2 2020]
- New improved MDQ Service [Q2 2020]
- Enhanced Community Attribute Profile support [Q2 2020]
- Improved support managing access to services per VO [Q2 2020]

- Support for AARC-G021 "Exchange of specific assurance information between Infrastructures" [Q3 2020]
- Support for AARC-G031 "Guidelines for evaluating the combined assurance of linked identities" [Q3 2020]
- Support for the updated version of AARC-G049 "A specification for IdP hinting" [Q3 2020]
- New OIDC frontend [Q3 2020]
- Improved IdP Registration flow [Q3 2020]
- Improved SP Management capabilities [Q4 2020]

2.5 INDIGO-IAM

2.5.1 Maintenance activities

Maintenance and evolution activities on IAM mainly focused on improving the following aspects of the service:

- Improved token exchange flexibility, with the development of token exchange policies which allow having fine-grained control on the token exchange process.
- Support for multiple token profiles, so that the same IAM instance can expose authentication and authorization information according to different token profiles. The token profile used is defined at the client application level.
- Improved management of Acceptable Usage Policies.
- Improved account lifecycle management.
- Introduction of support for the AARC G002 profile for group membership information.

2.5.2 Summary of service enhancements

The enhancements described in the previous section have been deployed in production for the communities served by INDIGO IAM.

2.5.3 Future plans

The main development task is the transition to Keycloak as the main IAM authentication engine. Keycloak is a flexible and popular open source solution by Redhat for centralized authentication and authorization. Integrating Keycloak in IAM will provide enhanced capabilities and improved sustainability. In this context, the following enhancements will be applied to Keycloak:

- **SAML federation support:** Keycloak already has rich support for SAML authentication mainly targeted at single SAML IDP enterprise use cases. The objective of this task is to extend this support to properly integrate with identity federations, i.e. support federation metadata validation and usable integration with a SAML discovery service in the Keycloak login page. [Q4 2020]
- **OIDC federation support:** The OpenID Connect federation standard will enable flexible and scalable trust establishment among entities and will represent a key enabling technology to either build identity federations on top of OpenID Connect or securely integrate with

existing ones. The objective of this task is to extend Keycloak to support the OpenID connect federation standard and demonstrate interoperability with other components/libraries currently in development in the context of the OpenID foundation. [Q4 2020]

2.6 Perun

A detailed description of the Perun service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

2.6.1 Maintenance activities

Main part of Perun maintenance activities are regular upgrades to the latest stable version to ensure the best user experience and access to new features for the users. On average, there are two releases, including minor ones, each month which all are deployed in the minimal time on the production infrastructure.

Vulnerability CVE-2020-5281 was reported for the Perun core component, which was immediately fixed and deployed. Perun instance for EOSC-hub does not use the feature in which the vulnerability was found.

There were no major outages of the service except the long-term outage of the monitoring system itself. According to the local secondary monitoring system and manual tests the service was operated without any issues.

2.6.2 Summary of service enhancements

Integration with eduTEAMS and Check-in services was improved. Better exchange of VOs and group information is now in place for Check-in service. With eduTEAMS, the focus was aimed mostly to improve registration flows, but there were some improvements in information exchange as well.

Configuration capabilities were enhanced which allows additional customization of the service for various environments.

User-facing features were improved as well. There were some minor changes in account linking flow, which will ease the procedure for users. First version of the life cycle of group membership is supported, but it will be further improved in the future.

2.6.3 Future plans

There are several user experience improvements planned which includes a completely new version of the user interface as well as improvement of other user-facing components. This is a long term plan which will be sequentially rolled out for individual communities based on their willingness to test the new features.

Additional improvements with other EOSH-hub AAI components are planned as well to enhance interoperability and improve user experience.

2.7 WaTTS

A detailed description of the WaTTS service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

2.7.1 Maintenance activities

WaTTS is maintained by a team of two people at KIT. Software extensions of the WaTTS service are developed by a different team that also comprises two people. The EGI demo and development instances have been added for authentication (in addition to the EGI and B2ACCESS production instances).

2.7.2 Summary of service enhancements

The service WaTTS is provided by a combination of software and hardware. The WaTTS software has been extended to support fault tolerance (FT) and high availability (HA). This was achieved by extending the WaTTS software with a native Erlang library, named mnesia [R18], so FT and HA can be supported. Support for high availability of the attached myProxy services was implemented via the unix tool lsync.

The hardware for HA operation is currently installed at KIT and is expected to be Operational in Q4/2020.

2.7.3 Future plans

Upgrade the hardware to operate in HA mode. The hardware (servers and racks) was ordered and shipped. The destination computer centre in KIT is currently undergoing reconstruction. One of the goals is to offer more general support for security requirements, such as those required by the credential store in WaTTS. Therefore, the installation is progressing slower than initially anticipated.

2.8 MasterPortal

The MasterPortal acts primarily as a caching intermediary service between end-services and the RCauth Online CA, thereby also hiding the complexity of certificate and key handling for those end-services. In a typical pure-webflow, the MasterPortal is seen by the end-users only as a 'redirect' between the end-service and the RCauth.eu online CA: authentication at the MasterPortal is effectively outsourced to that CA. Another use is providing proxy certificates on the commandline by using ssh-key authentication, where the public key can be uploaded to the MasterPortal.

A more detailed description of the MasterPortal service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

2.8.1 Maintenance activities

The code, which builds upon CIlogon code [R19], has been updated and is now based on the 4.2 stable upstream code. No known downtime.

2.8.2 Summary of service enhancements

The following service enhancements have been implemented:

- When using the ssh key API, you can now restrict it to a specific scope.
- It is now possible to manage clients (i.e. Science Gateways and VO portals) also using a JSON-based REST API (/clients) making use of special administrative client credentials.
- Using the new /revoke endpoint, clients can now revoke their own refresh tokens.
- it is now possible to configure a client to *only* receive limited proxies.
- VO-portal:
  - In addition to plain proxies, it is now possible to directly obtain VOMS proxies via the VO portal (not yet configured on the production instance).
  - By default, the portal now prints the user's username (sub claim). Additionally, you can also view the rest of the received claims (userinfo response).
- Ssh keys portal:
  - By default, the portal now prints the user's name (*name* or *given name+family name*), username and IdP's display name (which claims are used for each of these is configurable).

2.8.3 Future plans

The EGI MasterPortal instance will be reconfigured to run in high availability mode.

2.9 RCauth - Online CA

A detailed description of the RCauth - Online CA service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

2.9.1 Maintenance activities

The code, which builds upon CIlogon code [R19], has been updated and is now based on the 4.2 stable upstream code. No known downtime.

2.9.2 Summary of service enhancements

2.9.2.1 Multi-site setup of RCauth

- Key cloning
  - Hardware procurement is completed for the sites that needed it.
  - The Key Cloning task was not finished in the second year as originally planned, since the task was much more complex than originally foreseen. This subtask itself had to be broken down into a large number of sub-subtasks (about eighty of them). Roughly speaking, the first year of the project was spent getting agreement for a plan for key cloning that was acceptable to the international community, and the second year on implementing the prerequisites for this plan.
- Cross site database
  - Currently behind schedule. Expected to use VPN instead of VPC, at least in the short to medium term.

- Deployment
  - There are three categories of software which need to be deployed - RCauth specific (such as the delegation server), generic infrastructure (MyProxy, database), and everything else: deployment configuration, monitoring, and glue to connect HSMs.
- Operator communications setup in the keybase is now completed. The complexity within this task was partly the need for some participants to rekey their PGP keys, which is a slightly involved procedure if one wishes to avoid mistakes.

2.9.2.2 RCauth operations

- It is now possible to manage clients (i.e. MasterPortals) also using a JSON-based REST API (/clients) making use of special administrative client credentials.
- Using the new /revoke endpoint, clients can now revoke their own refresh tokens.
- it is now possible to configure a client to *only* receive limited proxies.

2.9.3 Future plans

Up until the end of the EOSC Hub project, the plan is to have a production high availability RCauth instance - provided by the three core sites - fully documented and retaining its accreditation in IGTF. Specifically, the coming quarters will require:

- Testing - more testing is needed to ensure that the database synchronisation works as intended, and that the service is consistent regardless of the endpoint.
- Documentation - for admins and integrators. Also, the end user documentation will likely need to be reviewed as part of other user documentation activities.
- Self-audit. As part of an IGTF accreditation, a CA is required to regularly self-audit, and present the results of this audit to the PMA. The self-audit should be annual, although the presentation to the PMA need not be annual - however, as RCauth has gone through significant change in EOSC Hub, it is necessary to present the results of an audit at the September 2020 PMA meeting.
- Some minor improvements may still be needed in the production setup.

2.10 Integration activities

2.10.1 Summary of integration activities

2.10.1.1 Integration of EOSC-hub AAI services

During the reporting period, the focus was put on the interconnection and the interoperability among the EOSC-hub AAI services. In this context, eduTEAMS was connected to B2ACCESS to allow research communities managed in eduTEAMS to access services and resources protected by B2ACCESS. Furthermore, the integration between B2ACCESS and Check-in was improved. Specifically, B2ACCESS disabled email verification for users authenticating with EGI Check-in (which already validates the email addresses of the users) to allow for a more seamless user experience the first time a user from Check-in is accessing a service behind B2ACCESS. For a detailed description of the alignment activities that were carried out during the reporting period and the implementation status for each EOSC-hub AAI service, please refer to Section 2.10.3.

2.10.1.2 Integration of EOSC-hub AAI with EOSC-hub Helpdesk

The EOSC Portal AAI, which is a part of the infrastructure layer of the EOSC-hub AAI, was connected to the EOSC-hub Helpdesk. This integration allows researchers to access the Helpdesk using the academic/social account of choice, including eduGAIN and the Community AAIs connected to the EOSC Portal AAI.

2.10.2 Identified integration gaps

The following integration gaps have been identified:

- **Multiple user registrations:** Users are asked to register with different AAI services as they access resources protected by different infrastructure proxies. The implementation of the remaining harmonisation activities will provide a more seamless user experience as researchers access resources across different domains.
- **Multiple IdP discovery steps:** As described in Section 2.1, the EOSC-hub AAI is based on the AARC BPA "community-first" approach, whereby users typically need to go through multiple IdP discovery steps: (a) to select their Community AAI and (b) to select their Home Organisation. During this process, users don't need to re-enter their login credentials as long as their Single Sign-On session is active, however the IdP selection can be frustrating in some cases. The "IdP hinting" protocol proposed in AARC-G049 [R20] can greatly simplify the discovery process for the end-user, by either narrowing down the number of possible IdPs to choose from or by making the actual selection process fully transparent.
- **OAuth2 token validation:** The current EOSC-hub AAI architecture works very well when the user is consuming services directly. However, there are use cases requiring a service agent to be able to act autonomously, on behalf of the user, consuming services and resources. If the services consumed by the agent are behind the same proxy, the current architecture works. For those cases, though, where an agent running on Service A needs to access resources on Service B, which might be connected by a different proxy, then there is no straight-forward solution at the moment. So, currently, services need to trust the same proxy to support those use cases. A solution for dynamically establishing trust in a distributed environment is provided by the OpenID Connect Federation specification v1.0 [R21]. The AARC community is working on "AARC-G052: Recommendations for OpenID Connect/OAuth2 token-based access across different infrastructures" [R22] that is meant to be a temporary measure until the OIDC Federation Specification is widely available. This interim solution is based on the OAuth2 Token Introspection specification [R23], which defines a method for a protected resource to query an OAuth 2.0 authorization server to determine the active state of an OAuth 2.0 token and to determine meta-information about this token.

2.10.3 Future plans

This section describes the future plans for the EOSC-hub AAI. These include alignment activities across the EOSC-hub AAI services which can be classified into technical and policy-related activities.

2.10.3.1 Technical alignment activities

Table 3-1 lists the identified technical alignment activities and their status. A green checkmark indicates a complete activity, otherwise the expected time of implementation is provided. The activities are detailed in the remainder of this section below.

Table 3-1 Roadmap of EOSC-hub AAI technical alignment activities

Activity	*B2ACCESS*	*Check-in*	*eduTEAMS*	*INDIGO-IAM*
Alignment of user attributes	✓	✓	✓	✓
Alignment of VO/group membership and role information	✓	✓	✓	✓
Alignment of resource capabilities information	✓	✓	✓	✓
Alignment of affiliation information	M30	M28	✓	M36
Alignment of assurance information (including freshness of affiliation information)	M36	M30	✓	M36
OAuth2 token validation across multiple domains (multi-proxy connection workaround)	✓	✓	✓	✓
OAuth2 token validation across multiple domains (initerim implementation based on OAuth2 introspection)	M30	M30	M30	✓

2.10.3.1.1 Alignment of user attributes

The attributes used to express user information should follow the REFEDS R&S attribute bundle, as defined in REFEDS-R&S [R24].

2.10.3.2 Alignment of VO/group membership and role information

VO/group membership and role information is typically used by relying parties for authorisation purposes. This information should be expressed according to the following syntax:

```
<NAMESPACE>:group:<GROUP>[:<SUBGROUP>]...[:role=<ROLE>]#<GROUP-AUTHORITY>
```

This syntax is detailed in the guidelines specified in AARC-G002 [R25].

2.10.3.3 Alignment of resource capabilities information

A capability defines the resource or child-resource a user is allowed to access, optionally specifying certain actions the user is entitled to perform. Capabilities can be used to convey - in a compact form - authorisation information. Capabilities should be expressed according to AARC-G027 [R26]:

```
<NAMESPACE>:res:<RESOURCE>[:<CHILD-
RESOURCE>]...[:act:<ACTION>[,<ACTION>]...]#<AUTHORITY>
```

2.10.3.4 Alignment of affiliation information

There are service providers that rely on affiliation information in order to control access to resources. Two different types of affiliation have been identified, namely *Affiliation within the Home Organisation*, such as a university, a research institution or private company; and *Affiliation within the Community*, such as cross-organisation collaborations. Affiliation information should be expressed according to AARC-G025 [R27] as depicted in Table 3-2:

Table 3-2 Alignment of affiliation information

Affiliation type	SAML attribute	OIDC claim
Affiliation within Community	`eduPersonScopedAffiliation`	`eduperson_scoped_affiliation`
Affiliation within Home Organisation	`voPersonExternalAffiliation`	`voperson_external_affiliation`

Note that AARC-G025 also provides guidelines for expressing the freshness of affiliation information. However, the expression of affiliation freshness will be covered as part of the alignment of assurance information activity (see Section 2.10.3.1.5).

2.10.3.5 Alignment of assurance information

Some service providers need to make authorisation decisions based on assurance information, which provides a means to express how much they can trust the attribute assertions about the authenticating user. The REFEDS Assurance framework (RAF) RAF-version-1.0 [R28] splits assurance into the following orthogonal components:

- the identifier uniqueness
- the identity assurance
- the attribute assurance

While the component values play the principal role in expressing assurance information, RAF supports composite profiles (`cappuccino` and `espresso` for example) which are the result of a specific combination of assurance components that need to be additionally asserted. The simplicity of exchanging a few well-understood profiles allows easier processing of assurance assertions by relying parties. RAF also specifies how to represent the assurance component and profile values using existing federated identity protocols, currently SAML 2.0 and OpenID Connect.

AARC has developed additional guidance that extend RAF:

- Guideline on the exchange of specific assurance information AARC-G021 [R29], which defines RAF-based profiles equivalent to `IGTF-BIRCH` and `IGTF-DOGWOOD`, and introduces `AARC-Assam`, a new specific profile addressing assurance partially derived from social-identity sources.
- Guideline for evaluating the combined assurance of linked identities AARC-G031 [R30], which describes how to evaluate the combined assurance when linking different identities and defines compensatory controls that allow BPA Proxies to obtain assurance information even when the IdP of the Home Organisation is lacking support for RAF.
- Guideline Expression of REFEDS RAF assurance components for identities derived from social media accounts AARC-G041 [R31], which describes how REFEDS RAF assurance components should be expressed by the BPA Proxies and how these may be combined on 'outbound' assertions, if the exchange involves authentications with credentials based on social media accounts (like Google, LinkedIn, Facebook, etc).
- Guidelines for expressing the freshness of affiliation information, as defined in AARC-G025 [R32] (see also Section 2.10.3.1.4).

2.10.3.5.1 OAuth2 token validation across multiple domains

There are use cases requiring a service agent to be able to act autonomously, on behalf of the user, consuming services and resources. If the services consumed by the agent are behind the same proxy, the EOSC-hub AAI architecture works. For those cases, though, where an agent running on Service A needs to access resources on Service B, which might be connected by a different proxy, then there is no straight-forward solution at the moment. So, currently, services need to trust the same proxy to support those use cases. As already stated in Section 2.10.2, the AARC community is working on "AARC-G052: Recommendations for OpenID Connect/OAuth2 token-based access across different infrastructures" [R33], which is meant to be a temporary measure until the OIDC Federation Specification [R34] is widely available.

2.10.3.6 Policy-related integration activities

Table 3-3 lists the identified policy-related activities and their status. A green checkmark indicates a complete activity, otherwise the expected time of implementation is provided. The activities are detailed in the remainder of this section.

Table 3-3 Roadmap of EOSC-hub AAI policy-related alignment activities

Activity	B2ACCESS	Check-in	eduTEAMS	INDIGO-IAM
Alignment of privacy statements	✓	M30	✓	✓
Alignment of operational security and incident response policies	✓	✓	✓	✓
Alignment of Acceptable Use Policies (AUPs)	M36	M30	✓	✓

2.10.3.6.1 Alignment of privacy statements

For the EOSC-hub AAI and for virtually all of the SPs, compliance with the GÉANT Data Protection Code of Conduct version 1 (DPCoCo-v1) [R35] is implicit, since it reflects the Data Protection Directive and means compliance with applicable European rules (see AARC-G040 [R36]). To explicitly declare compliance with DPCoCo-v1, the privacy notice of each EOSC-hub AAI service should include a reference to DPCoCo-v1.

2.10.3.6.2 Alignment of operational security and incident response policies

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) V.1.0 [R37] provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration. The entities of the EOSC-hub AAI registered with eduGAIN should meet the Sirtfi requirements and express Sirtfi compliance in their metadata in order to facilitate coordinated response to security incidents across organisational boundaries.

2.10.3.6.3 Alignment of Acceptable Use Policies (AUPs)

The acceptable use policy (AUP) and terms and conditions of an infrastructure bind the user to the purpose for which the services and resources are provided. The AUPs of different organisations, service providers, and infrastructures can vary significantly. To reduce the burden on the users and increase the likelihood that they will read the AUP as they access resources from multiple service and resource providers, the EOSC-hub AAI services should adopt the WISE Baseline AUP model WISE-AUP [R38]. This model includes a common set of criteria for acceptable use and terms and conditions which can be augmented with community- and infrastructure-specific terms and conditions.

2.10.3.7 Integration of EOSC-hub AAI services

This section presents the integration roadmap of the EOSC-hub AAI services. The status of each of the required integrations or the expected time of implementation is described in the table below. Integrations which have already been established are marked with a check mark.

Table 3-4 Roadmap of EOSC-hub AAI integration

	EUDAT	EGI	GEANT	INDIGO-IAM
B2ACCESS		✓	M36	M36
Check-in	✓		M36	✓
eduTEAMS	✓	✓		M36
INDIGO-IAM	M36	M28	M36	

3   Marketplace and Order Management tools

3.1 Overview

The EOSC-hub Order Management System (OMS) as shown in Figure 3-1 comprises several central components including the Service Catalogue and Marketplace (MP), Service Portfolio Management Tool (SPMT), Service Order Management Back Office (SOMBO) and integrates many other systems to facilitate promotion, discovery, access and ordering of the productional EOSC-hub services in the distributed EOSC environment.

The EOSC-hub OMS allow customers to access the central EOSC-hub Marketplace, discover services and resources using the intelligent search and filtering mechanism, place an order and track it until its fulfilment and service or resource delivery. The EOSC-hub OMS integrate Order Management Systems, which are operated by other e-infrastructures.
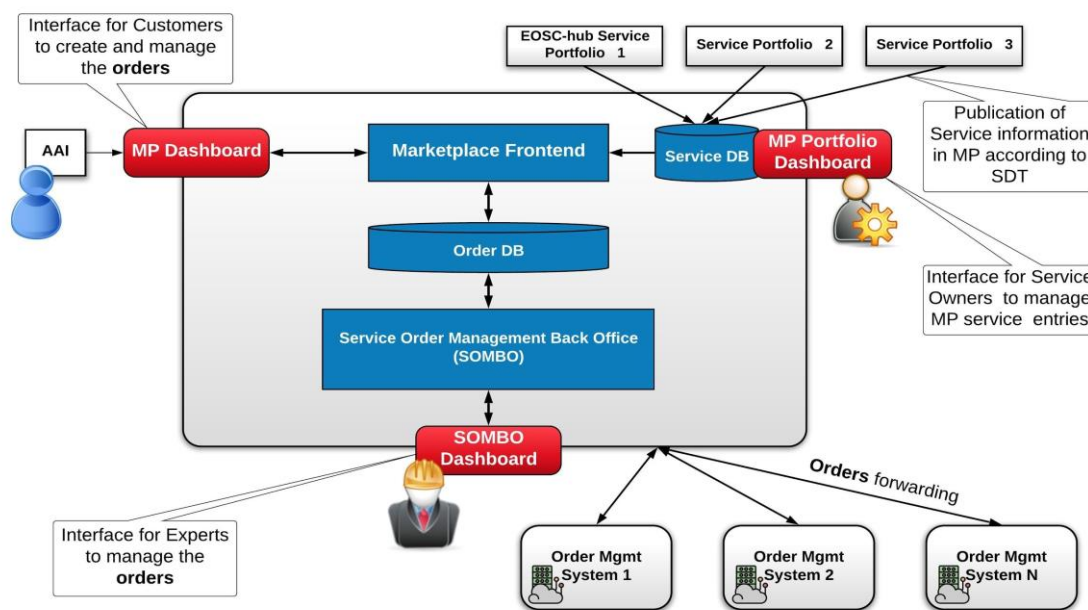
Fig.3-1 - EOSC-hub Order Management System high-level architecture

3.2 Marketplace

A detailed description of the initial version of Marketplace service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

3.2.1   Maintenance activities

In order to ensure high availability and platform's smooth operation, regular software updates including gems' updates are being performed.

3.2.2   Summary of service enhancements

During the last months, the Marketplace has been evolving in various dimensions. As it is the central platform in user-facing service delivery chain it must provide:

- Features to ensure proper service presentation and creation of service offers for the Service Organisations.
- User friendly environment for the service discovery and service ordering for the EOSC users.
- Integration with other EOSC-hub tools involved in service delivery to support surrounding processes

During this reporting period many activities were undertaken. Main features delivered for the EOSC users are:

- **Marketplace Projects** as a lightway approach to allow the user to organise their services and service orders into logical blocks to reflect a common purpose and gain support in the scope of the created project. It's ultimate goal is to provide a user-friendly and helpful UI where EOSC services of a user interest can be gathered and managed and the user is carried step by step through the service order management process at the same time being separated from the complex operational side of this process.
- **Service Access Types -** We improve the service access paths and we divided them into 3 categories:
    - **Open access** - services are open to everyone, no login required. The user is immediately redirected to the services and no orders are created. Access requests coming from EOSC-hub need to be tracked and stored.
    - **External ordering** - service orders are handled externally, but access requests coming from EOSC-hub can be tracked and reflected in the Management Back Office. Access to the service can be granted automatically after sending the request.
    - **Internal ordering** - identity of a user is required (user has to be logged in in the EOSC Portal to get access to the service). Service requires submitting a service request filled with information relevant from the provider's perspective. Access has to be granted manually after analysis of the request.
- Improvement of the user interface during user journey (content adjustment, FAQs page, more user-friendly information).
- Improvements in service offers (offer status, markdown rendering, offers parameter, JIRA transition).
- User feedback-based enhancements of service visibility and discoverability in the MP.
- Implementation of the helpdesk interface in Marketplace as a communication channel for general support of federated services.
- Marketplace Metrics for European Commission (Number of providers in the Marketplace, Thematic disciplines of users ordering services, Countries of users ordering services).

To support many requirements coming from WP4 (Federated Service Management) and better support Service Order Management (SOM) procedures many improvements and extensions in the tool chain MP - JIRA - SOMBO has been introduced, such as:

- Project-Orders hierarchy in JIRA which will be reflected with Epic-Task hierarchy model (master and sub-tickets)
- Improvements in notification mechanism about relevant events (for ex. ticket creation) for the roles involved in the SOM Procedure such as JIRA shifters

We also provided the API to make possible extraction of the service information (service owner contact email) for integration with SOMBO to facilitate the dispatching procedure being done by SOM crew on shift.

3.2.3 Future plans

Our plans in the short terms:

- Preparations for the Marketplace White Label solution (content and graphical customizability)
- Enhancements in service offer attributes - structured schema, relational architecture reflected in filtering and search capabilities

3.3 Service Portfolio Management Tool (AGORA)

The Service Portfolio Management Tool is a tool aimed at facilitating service management in IT service provision, including federated scenarios. SPMT represents a complete list of the services managed by a service provider; some of these services are visible to the customers, while others are internal. The service management system has been designed to be compatible with the FitSM service portfolio management [R39]. Figure 3-2 shows the top Web UI of the SPMT.

A detailed description of the SPMT service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

Fig. 3-2 EOSC-hub SPMT Web UI

3.3.1 Maintenance activities

There is a standardized maintenance window every first Wednesday and Thursday of each month. These maintenance windows are used for applying regular OS upgrades and stable releases. All necessary precautions (backing the data) are taken care of beforehand by the monitoring team.

One major part of maintenance activities is the updates / upgrades of the software / library dependencies the AGORA has. This follows a specific process where performance, features, and service stability are taken into consideration. When a reliable version of a software dependency is available, the development team deploys a new stand-alone instance to test the validity of all main features and decide on a list of changes required. When a stable version is implemented, it is deployed on the development instance for at least one month until it is deployed in the production service. AGORA follows an agile development process that includes mandatory tests for checking the functionality and the quality, correctness of the software. This process consists of automated unit tests and code quality checks, running via a CI tool (GitLab). Unit tests that test crud and domain logic functionality on all resource objects supported by the API.

3.3.2 Summary of service enhancements

In the last period we performed a number of fundamental changes in the model that AGORA uses in order to be compatible with the Service Description Template (SDT) version 1.1, 1.2 and version 1.3. We also made a number of improvements in the User interface in order to make it easier to use. (e.g. added autocomplete functionality for Tags, Organisations, Certifications etc.)

3.3.3 Future plans

Our plan for the next period is to adapt the model of Agora once more in order to add support for the new Service Definition Template, which is being developed with current version v2.10 in SPMT/AGORA and to proceed with the integration of SPMT with the EOSC - Portal as necessary. In more detail AGORA will perform the following actions

- Design & implement the Organisation Description Model from SDT v2.10
- Design & Implement the Service Description Model from SDT v2.10
- Design & Implement the relationship between Services.
- Design & Implement the relationship between Organisations.
- Design & Implement the relationship between Services & Organisations
- Design & Implement the relationship between Organisations & Possible communication methods (API, e-mail etc).

A prototype of the relationships between entities in the SPMT model is depicted in Figure 3-3 below.
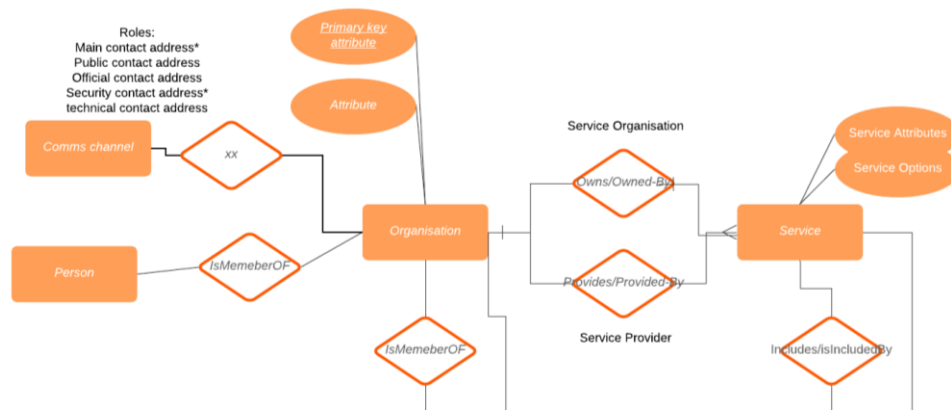
Fig.3-3 SDT Entities Relationship Diagram.

3.4 Integration activities

3.4.1 Integration of Marketplace with Service Order Management Back Office

3.4.1.1 Summary of integration activities

In the reporting period:

- We introduced the ticket hierarchy in JIRA (the new specification assumes that every project creates a master ticket with project dependent fields, and every ordered service has its own ticket related to the project ticket)
- We introduced new workflows for each type of tickets (master and sub-ticket) allowing to exchange information between the Customer and Operational Teams (First Line, Providers etc)

3.4.1.2 Identified integration gaps

We still need to introduce versioning to JIRA ticket workflows and templates. In this way it will be possible to smoothly move between the versions without any disruption to the MP users. To orderly manage this task, a JIRA schema versioning procedure has been proposed:

In case of introducing changes to any project related schema (workflow/ticket etc):

1. A dedicated JIRA project should be in place where new schemas are created and VERSIONED (via agreed naming pattern) - e.g. EOSCSOWORKFLOWS.
2. In case of a new schema, the info about the new schema should be propagated via CHANGELOG (for the beginning a confluence page would be sufficient), where all schema versions are listed with names, basic information about the changes and any other relevant comments).

3. A new version is connected to EOSCSODEV and <u>EOSCSOMASTER</u> projects (JIRA projects connected with MP and Ops Portal dev instances), where appropriate development takes place.
4. After integration with a new schema, moving changes up to EOSCSOSTAGING (common JIRA project for MP and COMBO integration).
5. Testing phase.
6. After positive testing results, moving to production to EOSCSO, which is a production project in JIRA.

3.4.1.3   Future plans

Next steps should focus on retrieving information about the SLA from the Ops Portal COMBO through JIRA. However, this functionality needs to be discussed in more detail.

3.4.2   Integration of Marketplace with EOSC Portal

3.4.2.1   Summary of integration activities

EOSC Portal developments implemented in the scope of a joint activity (Section JA3) defined in the EOSC Portal Collaboration agreement:
- Definition of EOSC Portal technical implementation architecture. Delivery of Portal architecture documentation.
- Definition and further development of a single portal (WUI) and entry point (API interface) for Service Providers to register and maintain service descriptions.
- Definition and/or further development of a single Service Database and the appropriate data APIs in which the service descriptions are maintained.
- Interconnection between the Service Database and the Portal User Interface.
- Optimisation of the integration of the current EOSC Portal, Service Catalogue and Marketplace and the APIs to improve the user experience.

3.4.2.2   Identified integration gaps

- The protocol used to communicate with eIC (eInfraCentral) EService Catalogue API should be refined to provide instant updates of service description
- The schema of service description (SDT) is still evolving, once this is defined the integration interfaces and underlying data schema need to be updated

3.4.2.3   Future plans

All integrations and features planned in the scope of JA3 have been delivered. EOSC Portal will be developed with emphasis on the user experience as a part of EOSC Enhance project. An appropriate methodology will be used to analyse the EOSC Portal user experience and then measure progress during implementation. This will result in describing personas and key usage scenarios.

Plans of the work:
- Establishment of methodology to be used to analyse the EOSC Portal user experience to measure progress during implementation

- Based on selected methodology creation of describing personas and key usage scenarios for each category (user journey)
- Gather feedback from task representatives for improvement and maintenance of the EOSC Portal
- Detailed analysis of the output
- Translate those requirements into operational models
- Coordination of aforementioned implementation of the requirements

4 Integrated Business and Operations Support Systems

4.1 Overview

This section details the maintenance and integration activities for the Operations Portal, GOCDB, DPMT, DMP and SVMON services. Significant enhancements have been performed for all services in the task addressing the requirements of the operational processes triggered in WP4.

The Service Order Management Back Office (SOMBO), with many enhancements, has been successfully deployed in production to be used for managing the order requests submitted in the Marketplace. The functionality introduced by SOMBO significantly simplifies the assignment and dispatching of the order requests to the Service Providers, improves the communication between all actors involved in the order enabling procedure and increases the efficiency of the SOM in general.

Many improvements have been done for configuration data repositories like GOCDB and DPMT. A first prototype of the EOSC centric dashboard has been developed for GOCDB. Significant improvement of presentation of complex topologies for distributed services has been implemented in the DPMT. Also, the accounting record provided by DPMT has been enriched with metadata of projects and communities associated with resources in use.

Still, the delays are observed in integration activities and implementation of the features requested by the EOSC Hub service order management process for distributed order management and configuration management. The delays are related to the significant, initially unplanned effort for migration of the services to the newer versions of frameworks and changes in infrastructure to guarantee the stable operation of the services. In addition, the complexity of adoption of order management systems developed by Service Providers to order management established in EOSC-hub Marketplace has to be considered.

4.2 Operations Portal

A detailed description of the Operations Portal service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.2 [R7].

4.2.1 Maintenance activities

The Operations Portal is composed of 3 components: a database, a web service and the php framework based on Symfony. In the last year we have several upgrades of these components to increase the performances and the efficiency of the global application.

The legacy version of the framework (based on symfony 1.4) has been removed and the application has been migrated on symfony 3.4. For the same reasons we have also upgraded several libraries (css and jss files) to improve performances.

4.2.2 Summary of service enhancements

Operations Dashboards

The management of user settings have been improved. There is also now the possibility to exchange information between on-duty operator teams with the use of handover logs.

SOMBO

Different enhancements have been done for the Service Order Management Back Office:

- An option to send a email to the user, when a comment is added into Jira.
- A role of shifter has been added to admin area in order to manage and update all issues registered in JIRA.
- Property for some fields to read-only in the summary of Jira issues.
- Adaption of the list to the new structure of Jira issues (epic or service order).
- Adaption of the workflow and the details to the type of ticket (epic or service order).
- Generation of the pages for service providers using tokens and sending email with the url to inform them.
- Generation of UID for service providers and service order to create hidden pages.
- A dashboard is now presenting issues sorted by status into a pie chart as shown in Figure 4-1.
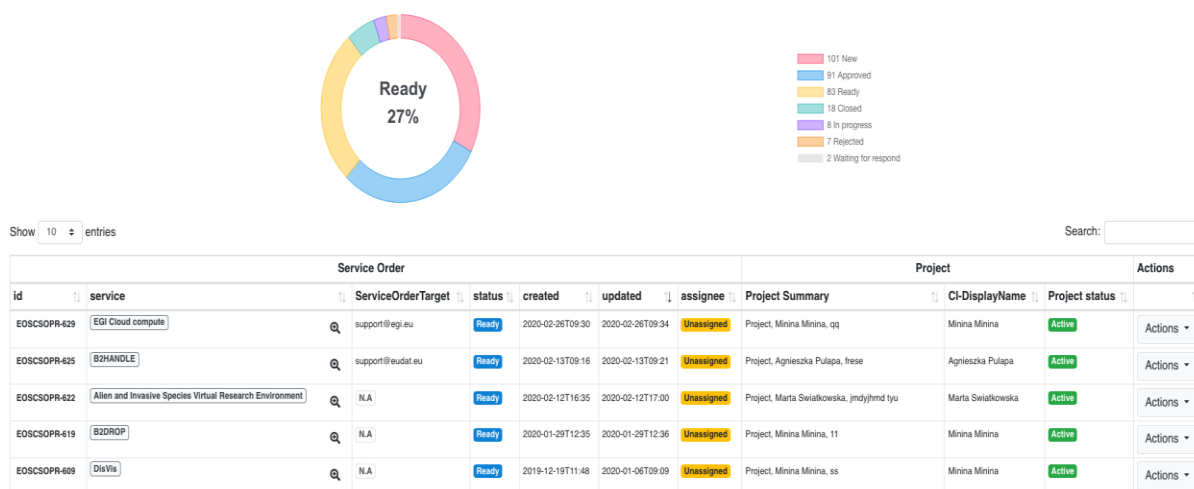
Fig.4-1 - Dashboard in SOMBO with status pie chart and list of orders

4.2.3 4.2.3 Future plans

- **Migrate to Symfony 5**

  Symfony is the framework used for the Operations Portal. The latest version is more flexible and provides new features which could improve the ecosystem used by Operations Portal. This upgrade requires a replacement of several deprecated libraries and classes.

- **Use EOSC AAI instead of EGI Checkin**

The EOSC AAI is more complete and provides access to more identity providers. This integration requires significant changes in the configuration of Operations Portal.

- **Improve VO ID card registration**

The VO module is a feature of the Operations Portal required by many communities and service providers. The registration of the VO should evolve:

  - To remove historical useless work-flows.
  - To add new possibilities of VO registries (CoManage for example).
  - To simplify the different forms for registration and update of the VO.
  - To provide more ergonomic tools and interfaces.

- **Integrate CoManage API**

The COmanage Registry is a new system able to register communities and groups like a VO. We will add a support into the VO ID card to ask for it and the possibility to register the information related to CoManage. But we also need to integrate the CoMange API to retrieve the list of users associated with a VO which is registered in CoManage.

4.3 GOCDB

A detailed description of the GOCDB service is given in D5.1 [R3]. The release notes for the reporting period are provided in D5.4 [R7].

4.3.1 Maintenance activities

Various bugs were fixed, including trimming white space from user submitted text fields, adding a "read-only" check to the Write API. We also improved our documentation and the depth at which knowledge is shared among the GOCDB team.

4.3.2 Summary of service enhancements

During the reporting period, we have introduced new features and fixed issues. First, we have enabled the GOCDB software to integrate with the EGI Check-In service using the new, AARC-G027 [R26] compliant, entitlement "out of the box". We have also refactored the Write API to make it more maintainable and extensible in future.

Development work has also been completed to allow for a first iteration of an EOSC view of GOCDB to be deployed internally to STFC as shown in Figure 4-2 below. The EOSC view will provide an EOSC centric look at the data already within GOCDB and will use the current Service Group functionality to represent EOSC federated services.
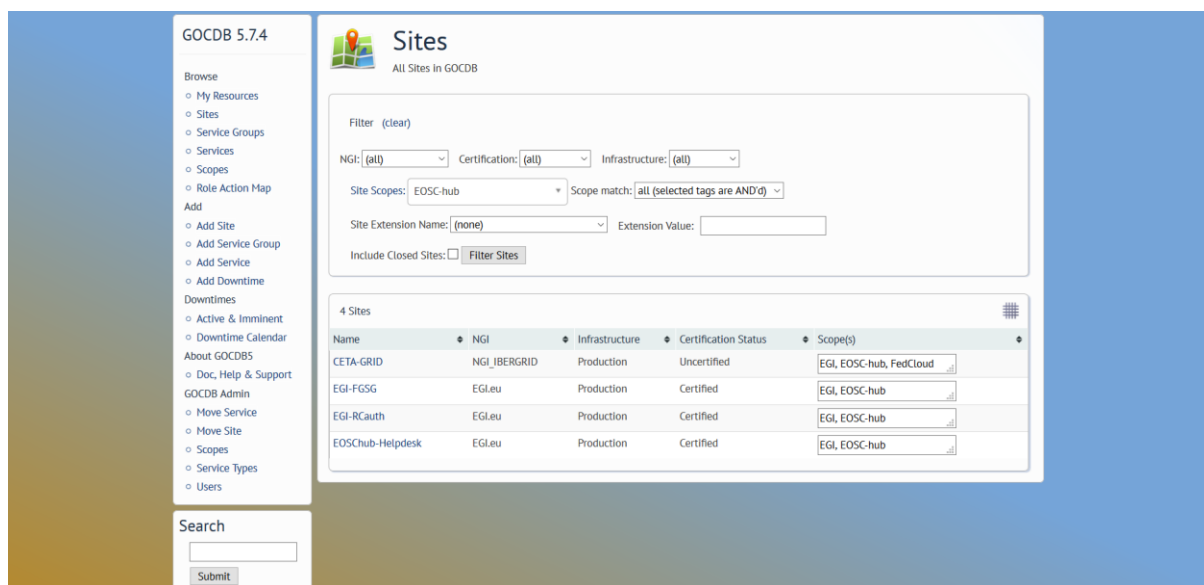
Fig.4-2 - GOCDB EOSC centric view

4.3.3 Future plans

- Update the version of the GOCDB software in production.
- Improvements will be made to how "Reserved Scopes" are handled by the GOCDB software.
- Creating new EOSC-hub specific ServiceTypes automatically when they are added to the EOSC-hub SPMT API.
- A second, configuration managed, production instance of GOCDB will be deployed behind our load balancer. This will not only increase the resilience and reliability of the GOCDB service, but also the long-term stability of the service, by allowing production instances of GOCDB to be brought online faster and with more guarantee that the configuration is correct.
- Over the course of the project, the failover instance will need to be moved to new infrastructure and placed under configuration management.
- The functionality of the Write API will be expanded to meet evolving use cases.
- Make the EOSC-hub view accessible via its own public URL.

4.4 Data Project Management Tool

A detailed description of the DPMT service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

4.4.1   Maintenance activities

General maintenance and operation have continuously been provided throughout the reporting period. No downtimes were required.

4.4.2   Summary of service enhancements

On the view of individual providers, a new tab has been introduced summarizing that provider's involvement grouped by activity type (responsible provider for a project, a registered service, a registered service component and registered storage resources).

For multitenant service components such as iRODS or Handle servers a dedicated and detailed endpoint model has been developed, implemented, and rolled out. This allows for a better description of the overall topology of more complex deployments as put in place by some providers. An example of the dedicated view is shown in Figure 4-3.

Fig.4-3 - Example of multitenant IRODS service component page

Note the endpoints offered by this iRODS server listed on the right-hand side. Clicking on any of these provides the configuration details of the respective endpoint.

The Storage Accounting Records (StAR views) exposed by DPMT for upstream consumption, e.g. by the EOSC Accounting Portal, have been enriched through the addition of further context information. Specifically, names and links to projects and user communities for individual storage resources have been added.

```
−<sr:StorageUsageRecord>
    <sr:RecordIdentity sr:createTime="2017-12-05T15:53:01Z" sr:recordId="accounting.eudat.eu/eudat/f931134d59424d768
    <sr:Site>EUDAT-BSC</sr:Site>
  −<sr:StorageSystem>
       https://dp.eudat.eu/providers/BSC/climatemodel-b2safe
    </sr:StorageSystem>
    <sr:StartTime>2017-12-04T15:53:01Z</sr:StartTime>
    <sr:EndTime>2017-12-05T15:53:01Z</sr:EndTime>
    <sr:ResourceCapacityUsed>159509138643</sr:ResourceCapacityUsed>
  −<sr:SubjectIdentity>
    −<sr:LocalUser>
        Institut Catal&#224; de Ci&#232;ncies del Clima (IC3)
     </sr:LocalUser>
      <sr:LocalGroup>Proj-ClimateModel-B2STAGE-B2SAFE</sr:LocalGroup>
    −<sr:UserIdentity>
        https://dp.eudat.eu/customers/institut-catala-de-ciencies-del-clima-ic3
     </sr:UserIdentity>
    −<sr:Group>
        https://dp.eudat.eu/projects/proj-climatemodel/proj-climatemodel-B2STAGE-B2SAFE
     </sr:Group>
      <sr:GroupAttribute sr:attributeType="title">Proj-ClimateModel-B2STAGE-B2SAFE</sr:GroupAttribute>
      <sr:GroupAttribute sr:attributeType="scope">EUDAT</sr:GroupAttribute>
    </sr:SubjectIdentity>
 </sr:StorageUsageRecord>
```

Fig.4-4- Example accounting record in StAR format

An example record in StAR format is shown in Figure 4.4. Take particular note of the user and group properties in the `SubjectIdentity` section. Non-ASCII characters are represented as HTML entities.

4.4.3 Future plans

So far, the DPMT application is based on the web content management system Plone version 4, thereby requiring Python 2. As Python 2 has reached end-of-life the entire application needs to be ported to Plone 5/Python3. Efforts have been increased to realize this in due time, but it turns out that the effort is substantial and so some delay is expected.

The migration mentioned above also includes several service enhancements such as the switch to SPMT API version 2 to collect information from the EUDAT Service Catalog. As the general migration to Python 3 is still ongoing some more specific enhancements that rely on this have to be delayed.

Interoperability with the EOSC Order Management and the Operations Portal were originally planned to happen peer-to-peer, exercising the DPMT's read and write REST API put in place before. In the meantime, it was decided to use the ARGO Messaging System instead. While a first draft of a suitable message format for the exchange of order information has been proposed further details still need to be defined. Specifically, the unique identification of services (including their components and options), customers, providers, and users across services remains an unsolved issue so far. Proposals to overcome this include a "meta registry" holding the information necessary to connect application-specific identifiers to corresponding entries in the various service components involved.

4.5 Data Management Planning Tool

A detailed description of the DMP service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

4.5.1 Maintenance activities

For the eestore service we have migrated the software to an upgraded service platform in Norway and have updated the service to harvest information for more external registries and extended the API (in some cases harvesting has required manual intervention as some third-party registries do not provide an API).

4.5.2 Summary of service enhancements

The openDMP service, which is now called ARGOS [R40] and is maintained and developed by openAIRE collaborators at the Athena research centre, Greece, has been deployed in production in the openAIRE framework.
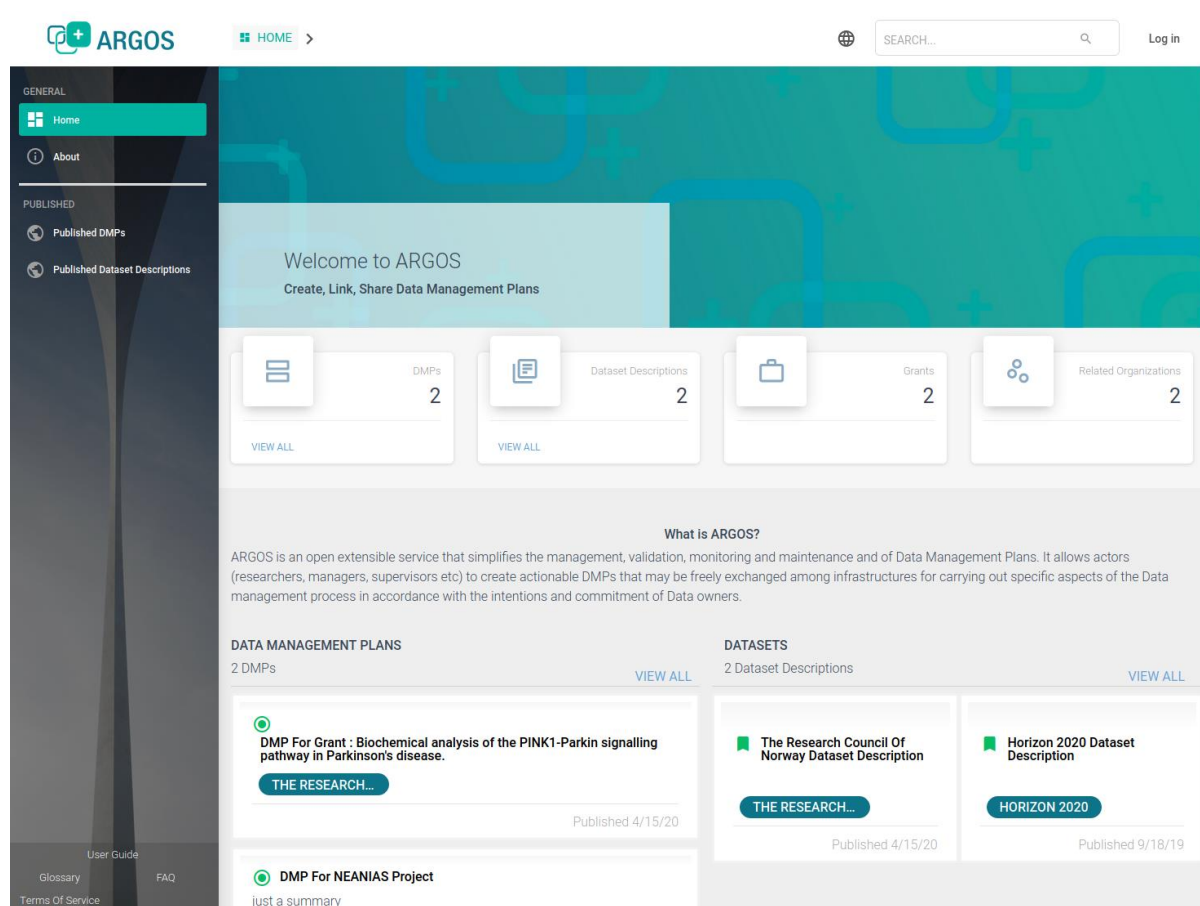

Fig.4-5 - Front-page of the ARGOS data management planning service

The Figure 4-5 shows a screenshot of the front-page of the ARGOS data management planning service.

During the Summer of 2019 a meeting took place in Garching to understand how to allow the eestore to harvest information from the DPMT and if it was possible to provide information to the DPMT from the data management plan to allow a service to be provisioned. We determined that it was not possible to provision services by passing information from the DMP plan to the DMPT due to the complexity of interoperating with the JIRA ticket system and the fact that the service requests would be handled through the EOSC-Hub Order Management system. We defined a means of enabling DMPT information necessary for a data management plan to be harvested (such as the storage services available to a given community). The first proof-of-concept was developed during the meeting that allowed information to be automatically harvested by the eestore.

4.5.3   Future plans

The next steps for the ARGOS service are to allow the plans to be published in the Zenodo service. This work will be mainly carried out by openAIRE collaborators. The eestore service will be updated to harvest plans from Zenodo such that they can be ingested into ARGOS. Further work on the integration with the DPMT will be carried out such that the eestore communicates with the DPMT through the Message Bus (see Figure 2-1 of D5.3) to harvest information on the available services. The eestore code will also be migrated from the deprecated Python 2 to Python 3.

4.6 Service Versions Monitoring Tool

A detailed description of the SVMON service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

4.6.1   Maintenance activities

The core back end of SVMON is based on Java Spring Framework connected with underlying MySQL Database operated in HA mode. The front end provided by Angular framework. The maintenance activities were focused on multiple bug fixes in both front and back ends. The Angular framework has been updated to the newer version 7.2.

4.6.2   Summary of service enhancements

During the second reporting period the representation of site information on the site dedicated page has been improved to a uniform view for both EGI and EUDAT sites. New version of HTTP API to get site information has been implemented. Another significant enhancement was the implementation of the token-based authentication for the svmon clients. This enhancement allowed secure communication and reporting of configuration information about services to the SVMON server. All clients deployed at services connected to SVMON have been updated.

Currently two installation options are available for SVMON clients:

- Standalone installation with token-based authentication
- Integrated installation with pakiti client without authentication

4.6.3 Future plans

The SVMON roadmap for the third reporting period will focus on provisioning of SVMON clients for EOSC core services like EOSC Portal, EOSC Marketplace etc. and the implementation of a dedicated dashboard which will provide the integrated view on major components of the core services, current software versions and history of updates. The SVMON client will be extended to include more supported service types.

4.7 Integration activities

4.7.1 Integration of Operations Portal with Marketplace

4.7.1.1 Summary of integration activities

As described in section 4.2.2 we have continued to improve the Service Order Management Back Office and its integration with the Marketplace, which is still based on the JIRA API layer.

To keep coherency between tools we need to use the same references especially about service providers. The Marketplace team has provided an API to gather all information related to service providers. This information is now reflected on the SOMBO part with the use of this API and significantly improves the order enabling procedure.

4.7.1.2 Identified integration gaps

Until now the work has been focused on exchanging information from the MarketPlace to SOMBO through the use of JIRA API and Marketplace API. We also need to ensure that some information is provided in return to the Marketplace like SLA or OLA between users and service providers.

The developed integration solution heavily relies on the JIRA system and has some constraints in scalability. It was agreed in EOSC-hub to migrate to ARGO Messaging Service (AMS) in the long term. Currently the required changes in interfaces of Marketplace and SOMBO are being assessed and evaluated. A clear roadmap and activity plan for migration to AMS is expected by the end of the project.

4.7.1.3 Future plans

Provide an API able to return all OLA / SLA signed between end users and service providers. Establish a plan for the migration to AMS.

4.7.2 Integration of Operations Portal with ARGO Messaging System

4.7.2.1 Summary of integration activities

Through this use of a plug-in of our web service we are able to publish and consume information within the ARGO messaging system.

The aim of this integration is to exchange information in a standard way with other order management systems. This integration requires the creation of a topic and then the order management system subscribes to this topic and SOMBO publishes on this topic.

This integration is completely generic. The envisaged usage is related to SOMBO and to the communication with different order management systems, but we can use it for any communication with third parties able to consume/publish information through AMS. The integration with AMS has been completed on the SOMBO side and SOMBO publishes information via AMS.

The Figure 4-6 is described an example of integration with 3 different order management systems which are exchanging information through AMS channel.
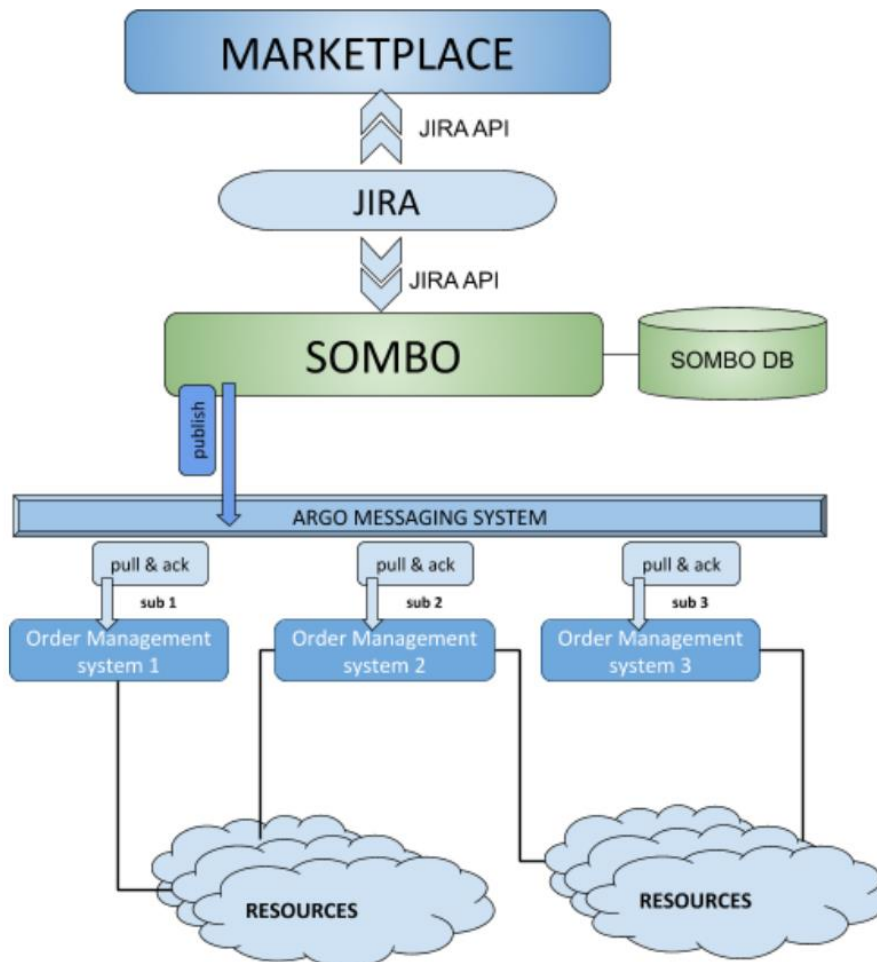
Fig.4-6 - High-level diagram of SOMBO integration with multiple Order Management Systems based on ARGO Messaging System

4.7.2.2   Identified integration gaps

No significant gaps in integration of SOMBO and AMS have been identified so far. But it's important to consider the complexity of integration of other order management systems with SOMBO. The analysis of DPMT integration shows that the integration requires significant efforts and was underestimated. The feasibility of this integration becomes less evident, taking into account the fact that most of the service providers do not have a mature order management system and that order management procedures are based in many cases just on helpdesk service.

4.7.2.3 Future plans

The integration of SOMBO with AMS is complete, the integration strategy with respect to the other service order management systems will be assessed and modified.

4.7.3 Integration of Operations Portal with DPMT

4.7.3.1 Summary of integration activities

Interoperability of DPMT with the EOSC Operations Portal was originally planned to happen peer-to-peer, exercising the DPMT's read and write REST API put in place before. In the meantime, it was decided to use the ARGO Messaging System instead. A first draft of a suitable message format for the exchange of order information has been proposed as illustrated in Figure 4-7:

```json
  ▼ additional: [
     ▼ {
           key: "request_type",
           value: "Development"
       }
     ],
     allowDiscussion: false,
     compute_resources: [ ],
     contributors: [ ],
     description: "For demonstration purposes only",
     endDate: "2022-03-31T00:00:00+00:00",
     expirationDate: null,
     id: "b2share-demo-request",
     identifiers: [ ],
     pid: null,
     portal_type: "ServiceRequest",
  ▼ preferred_providers: [
     ▼ {
           path: "providers/JUELICH",
           title: "JUELICH",
           uid: "7703449277cb4011972ef7223776f472"
       }
     ],
     registered_service: [ ],
     relatedItems: [ ],
     resource_comment: "<p>If applicable and already known how much r
     later).</p>\n",
     rights: "",
  ▼ service: [
     ▼ {
           path: "catalog/B2SHARE",
           title: "B2SHARE",
           uid: "d2cb1386f880484d9569342bc61f7d48"
       }
     ],
  ▼ service_hours: [
     ▼ {
           path: "services/SLA/a-level-service-time-08-16",
           title: "A level: service time 08-16",
           uid: "89b776138bf54e5aa22d501ef74f1298"
       }
     ],
  ▼ service_option: [
     ▼ {
           path: "catalog/B2SHARE/options/default",
           title: "B2SHARE: Default",
           uid: "7f3dd440b80b4f0fa06854842d2cc158"
       }
     ],
     startDate: "2020-04-01T00:00:00+00:00",
  ▼ storage_resources: [
     ▼ {
           "storage class": "online+",
           unit: "TB",
           value: "20"
       }
     ],
     subject: [ ],
     text: "<p>More explanatory text could go here</p>",
     ticketid: "12345",
     title: "B2Share Demo Request",
     uid: "f367ca818f7a4a98b7d2611a4b55ebc8"
 }
```

Fig.4-7 - A snippet of the message format for exchange of order information

JSON representation of an example request coded in the proposed message format. Note how cross-references to other - existing - entities are encoded here.

4.7.3.2   Integration gaps

When sending order information from the Operations Portal to DPMT it is not yet clear how to uniquely and unambiguously identify certain elements within the message such as services (including their components and options), customers, providers, and users.

4.7.3.3   Future plans

Proposals to overcome the gap mentioned above include a "meta registry" holding the information necessary to connect application-specific identifiers to corresponding entities in the various service components involved. The DPMT itself could be used here as it has intrinsic support for multiple identifiers built in. A decision on exactly how to proceed is still pending and will rely on a general integration strategy with respect to third order management systems as described in Section 4.7.2.2.

5 Monitoring, Accounting, Messaging and Security Tools

5.1 Overview

This chapter provides the maintenance and integration activities performed for the ARGO Availability and Reliability Monitoring Service, ARGO Messaging Service, Accounting Repository, Accounting Portal, and Security Tools. We also describe what the next steps are towards the integration plan for each tool/service.

5.2 Accounting Repository

The Accounting Repository service is implemented using a software collection known as APEL. APEL is a computer resource usage accounting tool that collects and stores compute (serial and parallel jobs), storage, and cloud resource usage data collected from Resource Centres of the EGI and EUDAT infrastructures. Accounting information is gathered from distributed sensors into a central Accounting Repository where it is processed to generate summaries that are then made available through the Accounting Portal.

A detailed description of the Accounting Repository service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R4].

5.2.1 Maintenance activities

There has been less need for maintenance this period thanks to the efforts in the last period to improve reliability and increase feedback from the systems. However, it is foreseen that there may be an increase in the maintenance required in the next period as a number of new systems are being brought online. This includes the full migration to using the ARGO Messaging Service (AMS) for exchanging accounting records and a new system to monitor the status of sites publishing accounting records.

As in the previous period, there have been a number of small bug fixes released for the APEL software this year. All the systems used to run the service have continued to be kept patched, and the latest IGTF Trust Anchor Distributions have been applied in a timely manner.

5.2.2 Summary of service enhancements

With a gradual move away from using BDIIs to publish information within the EGI and WLCG infrastructures, an option to update the APEL client benchmarks using a local configuration option has been added so that the APEL client is not dependent on the availability of a BDII.

A change was made to how virtual machines (VMs) that run for long enough to cross month-boundaries are handled in the accounting, so that, rather than keeping the record with the latest timestamp, the last received record for a VM in each month is kept regardless of timestamp. This simplifies sites republishing cloud VM accounting records as they no longer need to request the central Repository team remove records manually before they republish.

A full release version has now been produced of the SSM messaging software that supports the ARGO Messaging Service which will enable the APEL client and server to send records via AMS. This version is currently in limited production usage and will be rolled out fully by the end of the project. There have also been some changes to the SSM software to improve its reliability and ease of use, and the versions of Python that the software supports have been brought up to date.

5.2.3   Future plans

Alongside the full migration to using the ARGO Messaging Service (AMS) for exchanging accounting records, work is progressing on a new system to monitor the status of sites publishing accounting records. This will include work to ensure that all the APEL software is compatible with Python 3. Where completely new software is created such as for the new monitoring system, it is logical to create this with Python 3 compatibility from the start.

There is a plan to introduce support for CentOS 8 to the Universal Middleware Distribution and so testing of the APEL software against this operating system will be performed in the next period.

5.3 Accounting Portal

A detailed description of the Accounting Portal service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.2 [R7].

5.3.1   Maintenance activities

There were many maintenance activities, beginning with monitoring the SSM queues used to communicate with APEL and receive accounting data, and the loaders which put these data in the database, since those failed several times, without leaving any error logs, so manual checking was needed.

Also, database indexes needed to be created and maintained depending on the data present in the database, to make expensive queries faster. Since the Accounting Portal doesn't have to write to the database unless there is a daily update from APEL, these indexes can be set up proactively, without performance penalties on writing to the database.

Stale records were eliminated, especially in some cases where cloud sites sent negative values on some metrics.

Security certificates were renovated, and the accounting.devel-next instance was moved to the egi.eu domain.

Security was improved by strengthening the access limitations on some paths of the web server and changing passwords regularly.

5.3.2   Summary of service enhancements

There is a fully working release of the accounting portal that supports SAML and integrated with EGI Check-in waiting for review before being deployed into production. This new version will allow users without X.509 credentials to access privileged views in the portal after being logged-in through Check-in.

In parallel a special instance is being maintained to continue facilitating EOSC-hub integration at eosc-accounting.egi.eu, since this integration is expected to remove some basic functionality on some views of the portal to streamline it (e.g. VO handling). This instance allows those changes to be made without impacting existing requirements in the vanilla instance. There was some research on integrating these back on the production portal but are pending until new requirements are obtained. The Tier2 PDF report was improved on some edge cases that impacted legend layouting, which defines the layout or position in the display or physical page of an element in relation with the other ones.

5.3.3 Future plans

The EOSC-hub integration will be further enhanced in the new EOSC instance when improved EUDAT requirements and data are available.

A new WLCG view to integrate pledge data with WLCG accounting will be done as a first step to later integrate Tier 1 and Tier 2 data in the same view.

Further security improvements will be implemented, including a new credential mechanism.

5.4 Argo Service Availability and Reliability Monitoring

Service Availability and Reliability Monitoring is a key service needed to gain insights into an infrastructure, the applications, services, and even into processes/behaviours. ARGO monitors services by emulating typical user scenarios which allows to infer the quality of service the actual user gets. It mimic's the actual end user behaviour without requiring special privileges or special configurations from the service provider side. As a result, ARGO offers near real-time status updates which allow both end-users and site admins to have an overview of the service offered at any given point in time. The major objective of the monitoring system is to quickly identify and correlate problems before they affect end-users and ultimately the productivity of the services, the infrastructure and finally the organization.
A detailed description of the ARGO monitoring service is given in D5.1 [R3]. The release notes for the reporting period are provided in D5.4 [R7].

5.4.1 Maintenance activities

There is a standardized maintenance window every first Wednesday and Thursday of each month. These maintenance windows are used to apply regular operating system upgrades and stable releases. All necessary precautions (backing up the data etc) are taken care of beforehand by the monitoring team.

ARGO follows a development process that includes mandatory tests for checking the functionality and the quality, correctness of the software. This process consists of automated unit tests and code quality checks, running via a CI tool (jenkins). The argo team maintains a full replica of the production deployment (devel, staging instance) that is used for development, testing and integration validation of all the components that ARGO comprises (mon, poem, compute engine, UI).

5.4.2 Summary of service enhancements

ARGO Monitoring is a flexible and scalable framework for monitoring the status, availability and reliability of services provided by infrastructures with medium to high complexity. It uses the latest technology trends (etc apache flink, apache hdfs) as its main components to support Big Data analysis (transfer, store, stream, transform, analyse) and to offer near real time alerts. ARGO Monitoring is successfully used by both EGI and EUDAT infrastructures. Based on all these the work on the project has been focused on the development of the following features:

- A **unified web-portal** that will combine services from a number of different providers/infrastructures (work in progress).
- **Customer defined thresholds** which provide the ability to define custom thresholds for specific services/metrics/sites (for example to monitor the requirements of an SLA). This give us the flexibility to provide different SLA targets to customers (e.g. different acceptable response time for a specific customer)
- **One Stop Shop** that simplifies and automates the operation and configuration of ARGO components so that it is able to update the data of existing tenants or to create and deploy new tenants, metrics, profiles by using the Argo Admin portal.
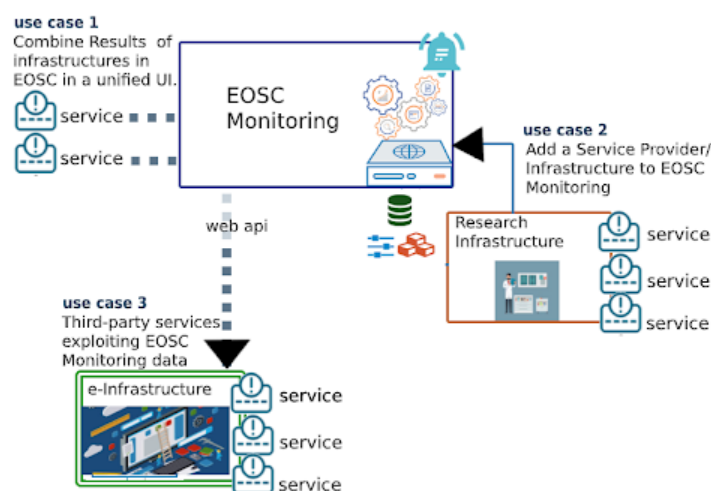
Fig.5-1 - Integration scenarios of the services in the EOSC ARGO Monitoring system

The main achievements for ARGO are the following:
a) Integration with the EOSC Portal
b) Enriching the One Stop Shop to allow ARGO to fulfil the following integration Use Cases as shown in Figure 5-1:
   ○ Use Case 1: Combine Results of one or more infrastructures in EOSC in a unified UI.
   ○ Use Case 2: Add a Service Provider/Infrastructure to EOSC Monitoring
   ○ Use Case 3: Third-party services exploiting EOSC Monitoring data
c) Development of ARGO Web-API as the main source of truth for all components instead of reading from different sources. This simplifies the process to add a new source of truth to ARGO (such as a new topology provider).

d) POEM is the new web UI that plays the role of the administrative component for managing packages, metrics, probes, reports and profiles. As a backend it uses the WEB-API to store the information.

e) A new public view of Services and Metrics associated with service types. This is a result of Service Integration with SPMT as the source of truth for Services and the Corresponding Service Types.

5.4.3   Future plans

Continue to develop the One Stop Shop, Customer Defined Thresholds and Unified UI features for ARGO namely develop a management interface to manage Customer Defined Thresholds and develop the ability to combine results for services regardless of the tenant they belong to.

5.5 ARGO Messaging Service

The ARGO Messaging Service (AMS) is a real-time messaging service that allows you to send and receive messages between independent applications. It is a Publish/Subscribe Service, which implements the Google PubSub protocol. Instead of focusing on a single Messaging API specification for handling the logic of publishing/subscribing to the broker network the API focuses on creating nodes of Publishers and Subscribers as a Service. It provides an HTTP API that enables Users/Systems to implement message oriented service using the Publish/Subscribe Model over plain HTTP as shown in Figure 5-2.
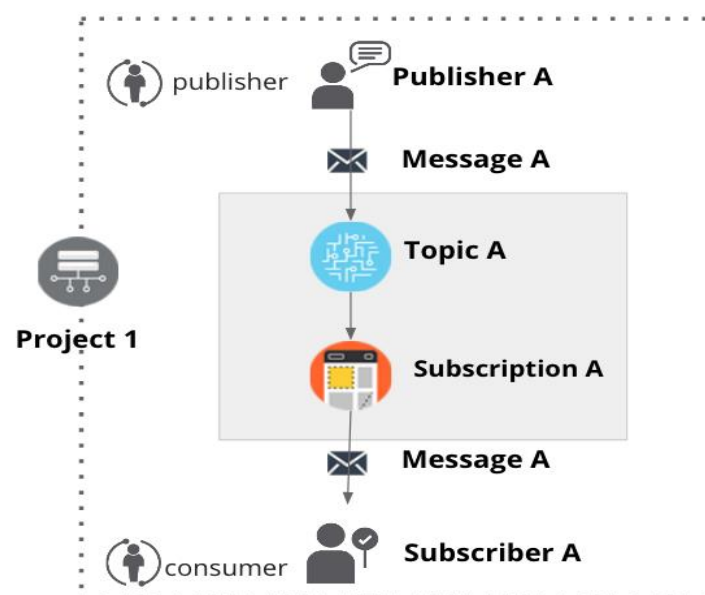

Fig.5-2 Publish/Subscribe Messaging Service

Features

- **Ease of use**: It supports an HTTP API and a python library so as to easily integrate with the AMS.

- **Push Delivery**: AMS instantly pushes asynchronous event notifications when messages are published to the message topic. Subscribers are notified when a message is available.
- **Replay messages**: replay messages that have been acknowledged by seeking a timestamp.
- **Schema Support**: on demand mechanism that enables a) the definition of the expected payload. schema, b) the definition of the expected set of attributes and values and c) the validation for each message if the requirements are met and immediately notify the client.
- **Replicate messages on multiple topics**: Republisher script that consumes and publishes messages for specific topics (e.g. SITES).

Architectural aspect

As shown in Figure 5-3, the current deployment of messaging service comprises a haproxy server, which acts as a load balancer for the 3 AMS servers running in the backend. This deployment offers

- **Durability**: provide very high durability, and at-least-once delivery, by storing copies of the same message on multiple servers.
- **Scalability**: It can handle increases in load without noticeable degradation of latency or availability
- **Latency**: A high performance service that can serve more than 1 billion messages per year
- **Availability**: it deals with different types of issues, gracefully failing over in a way that is unnoticeable to end users. Failures can occur in hardware, in software, and due to load.
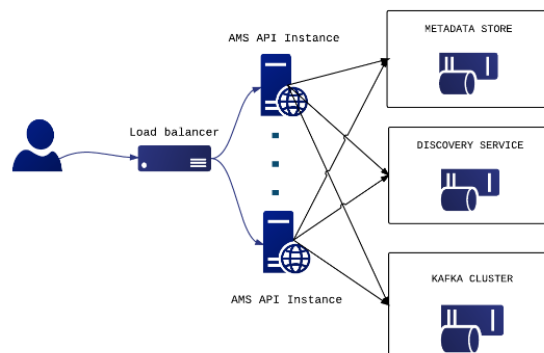
Fig.5-3 Deployment of messaging service

It supports both push and pull message delivery. In push delivery, the Messaging Service initiates requests to your subscriber application to deliver messages. In pull delivery, your subscription application initiates requests to the server to retrieve messages.

Apart from all these the Messaging Service supports:

- Argo-ams-library: A simple library to interact with the ARGO Messaging Service.

- Argo-AuthN: Argo-authn is a new Authentication Service.

- AMS Metrics: Metrics about the service

An initial description of the ARGO messaging service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

5.5.1   Maintenance activities

There is a standardized maintenance window every first Wednesday and Thursday of each month. These maintenance windows are used for applying regular OS upgrades and stable releases. All necessary precautions (backing up the data etc) are taken care of beforehand by the monitoring team.

One major part of maintenance activities is the updates / upgrades of the software / library dependencies the AMS has. This follows a specific process where performance, features, and service stability are taken into consideration. When a reliable version of a software dependency is available, the development team deploys a new stand-alone instance to test the validity of all main features and decide on a list of changes required. When a stable version is implemented, it is deployed on the development instance for at least one month until it is deployed in the production service.

AMS follows a development process that includes mandatory tests for checking the functionality and the quality, correctness of the software. This process consists of automated unit tests and code quality checks, running via a CI tool (jenkins). Unit tests that test crud and domain logic functionality on all resource objects supported by the api, using mock interfaces on the datastore and broker layers (golang testify). At the same time AMS endpoints are tested as postman collections via newman. Newman is a command-line collection runner for Postman [R42]. This allows the user to effortlessly run and test a Postman Collections [R43] directly from the command-line. It is built with extensibility in mind and it can be easily integrated with ARGO's continuous integration server and build systems.

5.5.2   Summary of service enhancements

The new implementation for the push server(s) has been deployed during the second reporting period. An initial prototype was ready during the first year and now the push functionality is fully decoupled from AMS api nodes. The push server(s) are an optional set of worker-machines - deployed on demand - that are needed when the AMS wants to support push enabled subscriptions. They perform the push functionality for the messages of a push enabled subscription (consume->deliver->ack). The new implementation provides a gRPC interface in order to communicate with AMS api [R44].

The Argo Messaging Service now supports Schema Validation per topic. This mechanism allows the user to define a schema for each topic and validate messages as they are published. This optional feature can protect topics from garbage or incomplete messages and may prove useful when a topic has multiple remote publishers to ensure data integrity on the client side. In order to support the development process this mechanism is also available as a "sandbox" api call.

In parallel we released Version 0.5.1 of the AMS Library that adds support for Python versions 3.4 and 3.6 (with *backwards compatibility)* running on CentOS 6 and CentOS 7. We have also implemented a number of new features of the AMS API and a retry mechanism if a message is not delivered due to network issues.

Finally, Operations portal integration was finalised that publishes and consumes information within the ARGO messaging system as was reported in Section 5.7.2 in more detail. The aim of this integration is to exchange information in a standard way with other order management systems

5.5.3   Future plans

ARGO Messaging future plans

- Enable limited user management support at the project level (Project admins will be able to add or remove users from a project)
- Allow user registration to the AMS Service and to a project. User's may register with the service and admins may accept or decline the registration.
- Adding bookmarks /snapshots on specific subscription offsets by capturing the current state.
- We are also investigating new features (google pub/sub new features) [R45] that will facilitate the use of AMS from new services.

Support the users the services that want to start or continue using the service such as:

- Support, maintain, extend the AMS Service, AuthN Service, ams-library

- Support FedCloud Information System, EGI Information System, AppDB

5.6   Security Tools: Pakiti

Pakiti provides a monitoring mechanism to check the patching status of Linux systems. Pakiti uses the client/server model, with clients running on monitored machines and sending reports to the Pakiti server for evaluation. The report contains a list of packages installed on the client system, which is subject to analysis done by the server. The Pakiti server compares versions against other versions which are obtained from various distribution vendors. Detected vulnerabilities identified using CVE identifiers are reported as the outcome, together with affected packages that need to be updated.

A detailed description of the Pakiti service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

5.6.1   Maintenance activities

The service was operated in accordance with the users' needs and without significant issues reported. The maintenance activities involved mainly applying updates both for the application and the operating system. User support was provided as part of the activities, too.

Preparing for a major update to the new version was postponed in order to address properly aspects that appeared during the evaluation phase. The transition is planned to be finished by the end of the project.

5.6.2   Summary of service enhancements

The work focused mainly on adaptations of the new Pakiti server. The implemented changes add new features to the graphical user interface and extend the command suite. A number of optimizations were implemented, and codebase re-engineered to ease the code maintenance.

5.6.3   Future plans

Finalizing the transition to Pakiti3. Ongoing maintenance and operations of the service will proceed.

5.7 Security Tools: Secant

Secant is a security cloud assessment framework that is used to check the security characteristics of virtual machines and their images. The framework instantiates the machine in a contained environment and runs a set of security probes against it. The probes combine external and internal checks and aim at typical configuration errors or vulnerabilities commonly misused by Internet attackers.

A detailed description of the Secant service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

5.7.1   Maintenance activities

The service closely relies on the underlying cloud fabric that is used to instantiate the virtual machines to test. Since the environment moved from OpenNebula to OpenStack it was inevitable to implement significant changes in the layer responsible for the machine management as well as prepare the setup allowing for proper image management. The main issue observed here is the missing full integration with the CloudKeeper for OpenStack.

5.7.2   Summary of service enhancements

The code was adapted to the OpenStack API, which makes it possible to use OpenStack as the testing platform.

5.7.3   Future plans

Switching the current pilot instance to full production usage is planned by the end of the year.

5.8 Integration Activities

5.8.1   Integration of Accounting Repository and Portal with EUDAT Accounting Service

5.8.1.1   Summary of integration activities

The EUDAT Accounting View started as a way to integrate EUDAT's storage accounting data into the regular Storage View. This started with a sample of data from EUDAT that was mapped into Storage Accounting Records (StAR). Since there was no formal topology of EUDAT sites available, the Portal had to generate that manually, along with transforming the data to ensure it conformed to the data types specifications.

5.8.1.2   Identified integration gaps

After performing a pilot, some differences in the semantics became apparent. EGI and WLCG accounting data is based on a consumption model, refreshed regularly and allowing averaging across dates and organizational variables. In contrast the data in EUDAT is updated irregularly, manually and uses a reserved space model, so that the data is sparse, and no averaging can be done. Support for units other than the terabyte had to be re-added, as the metric used in the data was previously deprecated. Another difference was that in the EUDAT data, dates indicate the moment a manual update occurred and not when the measurement was taken.

5.8.1.3   Future plans

Due to the sparse nature of the EUDAT data and the semantic differences, it may be better to present a static report page alongside the other views of EGI/WLCG data. In principle, this should better present the data by not interpreting missing data as a zero, avoid mixing dates with different definitions, remove the need to aggregate sparse data beyond what is sensible. The report can simply list the last reserve values for a given time period. More requirements are expected in the future.

5.8.2   Integration of ARGO with EOSC Portal

5.8.2.1   Summary of integration activities

ARGO has a pilot integration with the EOSC portal and uses the topology it provides to monitor the service listed and provide a view of their status at [R41] . The main goal is to check the validity of the services onboarded in the portal and identify "dead" services. Through the Web UIl operators, customers and providers can now check the health status of a service and get information about its stability.

5.8.2.2   Future plans

This was a pilot to try out one of the use cases and it highlighted the work that still needs to be done in order to complete the One Stop Shop task.

6 Helpdesk Services and Tools

6.1 Overview

This section details the maintenance and integration activities for the EOSC Helpdesk system together with integrated EGI and EUDAT helpdesks. The deployment of EOSC helpdesk and its integration with the EGI and EUDAT helpdesk systems has been accomplished in the previous reporting period and has been reported in detail in [R13]. The focus during the current reporting period was given to integration of the EOSC Helpdesk with EOSC Portal, Marketplace and improvement of the structure of the Support units to meet the requirements of the Incident and Service Request Management Process.

6.2 GGUS

A detailed description of the GGUS messaging service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

In addition, information on change, release and deployment are available in the EGI wiki at [R46] [R47].

6.2.1 Maintenance activities

GGUS releases take place in a bi-monthly release schedule. Releases are usually done on the last Wednesday of the release month. They are recorded and announced via GOC DB maintenance feature. All release dates are listed in EGI wiki. No major changes during the covered period have been performed. Maintenance activities of GGUS are documented in the GGUS release notes available at [R48].

6.2.2 Summary of service enhancements

The following enhancements have been implemented during the second period of the project:

- Enabled report "violated response time".
- Improved export of CSV/XML search results.
- Granted GGUS support privileges for members of ggus-supporters in EGI AAI.
- Implemented email validation and sanitization.
- Improved mailparser for recognizing external ticket IDs.
- Improved VOMS synchronization.

6.2.3 Future plans

No significant further enhancements or integrations planned for the next reporting period.

6.3 EUDAT-RT

6.3.1 Maintenance activities

No major changes during the covered period have been performed.

6.3.2 Summary of service enhancements

Information was added on the first page of heldpesk.eosc-hub.eu for information about the statues of tickets. Along with this, a link to "My support units" page was introduced for helping the 1st level but also the user to add the ticket to the correct unit. Also, information was added about the ticket cycle.

6.3.3 Future plans

Information will be added for the users and the 1st level explaining the hierarchy of the support levels. The support units will also include better descriptions of the supported activities in order to give hints on which problem should be assigned to the correct support unit for quicker categorization.

6.4 xGUS

The helpdesk service for EOSC-hub project is managed by xGUS. The service is available at heldpesk.eosc-hub.eu and it is open to any user with an account on B2ACCESS or Check-in. The users can submit to xGUS any request related to services from EOSC-hub or any infrastructure under the umbrella of EOSC-hub as EUDAT or EGI.

6.4.1 Maintenance activities

Maintenance activities are coupled with GGUS maintenance activities. About xGUS releases, they take place in a bi-monthly release schedule. Releases are usually done on the last Wednesday of the release month. They are recorded and announced via GOCDB.

6.4.2 Summary of service enhancements

The integration of the EOSC-hub helpdesk in EOSC AAI has been accomplished. The previous authentication via x509 certificates has been disabled. The field "Ticket category" has been added to the ticket template.

6.4.3 Future plans

For the xGUS instance used at EOSC-hub project the future tasks will be focused in the improvement of the usability for the end user, and the adaptation of the graphical interface with the current EOSC-hub public image. Also in the connectivity of xGUS with other ticketing systems used at EOSC-hub level, we are working on the possibility to move requests from xGUS to the JIRA used for tracking requests in the internal services (this point is in study from the xGUS developers at KIT to understand its feasibility)

6.5 Integration activities

6.5.1   Integration of xGUS with EOSC Portal and Marketplace

6.5.1.1   Summary of integration activities

The integration of the Helpdesk with EOSC Portal which has been accomplished according to the roadmap exposed in previous deliverables, provides the unique point of access for users and customers of EOSC to submit incidents, make service requests by filling the webform without any authentication or registration procedure. This passwordless approach significantly reduces a communication barrier between users and service providers of EOSC.

In addition the same integration has been done in the Marketplace by implementing pop-up UI available on all pages to simplify the access to support for the users at any stage of the ordering process. Both helpdesk interfaces in EOSC Portal and Marketplace are shown in Figure 6-1:

a)   b)

Fig.6-1 **Helpdesk forms for support requests: a) in EOSC Portal; b) in Marketplace**

6.5.1.2   Identified integration gaps

The integration gap related to ticket categorisation reported in D5.3 has been fixed. No further integration gaps have been identified.

6.5.1.3   Future plans

The future plans are focused on maintenance work of the EOSC helpdesk system and further improvement and extension of support units, providing the helpdesk as a service for the support teams of the onboarded services upon request.

7 Application store, Software Repositories and other Collaboration Tools

7.1 Overview

This section details the maintenance and integration activities for the Application Database, Software Repository and GitLab instance, along with enhancements made and plans for the future. The AppDB and its VMOps dashboard have received a major overhaul in order to support GLUE2.1 and OIDC authentication. The AppDB Information System which they rely upon for site and resources discovery got reworked as well, along with its public API. The Software Repository gained support for a new major UMD version and the latest release of CentOS. GitLab's operation is stable and saw a significant increase in usage.

7.2 Application Database

A detailed description of the AppDB service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

7.2.1 Maintenance activities

During the second year of the project, the AppDB portal received one minor and five revision releases, starting with 6.1.13, up to 6.2.2. Apart from some service enhancements addressed in the following sections, these releases addressed a variety of fixes pertaining to security and usability of the service, as well as other routine bug fixes.

7.2.2 Summary of service enhancements

AppDB is composed of several components and services that work together, sharing data and complementing features. One of the changes that took effect and was relevant to all AppDB components was the introduction of the GLUE2.1 schema with provisions for cloud computing and the FedCloud shift towards OpenID connect and OpenStack, versus x509 and OCCI/OpenNebula. In order to support these new trends, the AppDB portal wasextended with support for VM images from site endpoints exposing native APIs (e.g. OpenStack) along with OCCI-enabled ones, support for site administrators of sites with org.openstack.nova endpoints to retrieve VO wide image lists, and preliminary support for GLUE2.1. Moreover, the AppDB Information System support for GLUE2.1, which is at the heart of the rest of the components, was improved and the VMOps dashboard also gained preliminary support for sites with native API endpoints as well as preliminary support for OpenID connect based authentication of user actions. All these interrelated service enhancements are available on the development instances of the services and will be released in tandem once deemed production-grade.

Another enhancement specific to the VMOps dashboard was the support for predefined per-user VO quotas as shown in Figure 7-1. Without a dedicated service to provide site resource availability for each VO at any given time, issues with users trying to deploy a VM from VMOps may arise,

leading to errors from sites about its resource quotas being exceeded. To minimize such errors, a new functionality was developed for the VMOPs dashboard, where each VO can have a predefined set of resources to provide to each user. There are three main resource types managed by the VMOps dashboard; CPU cores, memory, and block storage. If a user has exceeded or is about to exceed these constraints the VMOps dashboard does not allow the deployment and suggests that the user undeploys one or more VMs in order to release resources. At the moment, the production instance of the dashboard supports quotas for the demo.fedcloud.egi.eu and vo.access.egi.eu VOs.
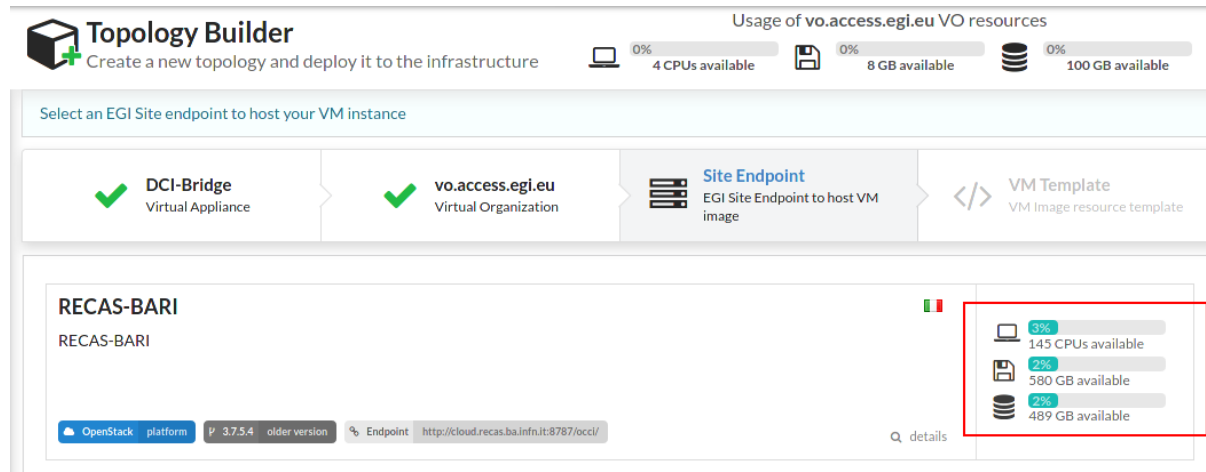

Fig.7-1 VO resource usage for the user (top) and
VO resource availability on selected site (bottom-right)

7.2.3   Future plans

The main plans for the AppDB portal and related services are focused on finalizing GLUE2.1/OIDC support and releasing the related upgraded components into production. Dropping OCCI support from the VMOps dashboard will follow suit, after sites get enough time to prepare for the migration. Other plans include the delivery of the VM Security dashboard and the VM Endorsement dashboard, which is already under development.

7.3 GitLab

GitLab instance provided by KIT is available to many resource communities and scientific organisations across Europe. During the second period of the project the significant increase of the active users has been observed. Currently the GitLab is actively used by ca. 300 users with steady increase and facilitates a full software development cycle for many scientific and infrastructure services.

A detailed description of the GitLab service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.4 [R7].

7.3.1   Maintenance activities

Regular updates according to the official GitLab release schedule. Stable operation of the service without any interruptions during the whole project period is observed. Daily backups of the GitLab instance as well as additional backups of GitLab database.

7.3.2 Summary of service enhancements

The GitLab runners are provided and being used by the developers.

7.3.3 Future plans

No further significant enhancements or integrations of the GitLab are planned till the end of the project.

7.4 EGI Software Repository

A detailed description of the EGI Software Repository service is given in D5.1 [R6]. The release notes for the reporting period are provided in D5.2 [R7].

7.4.1 Maintenance activities

Apart from the usual support activities, maintenance activities during the period in question include resolving some issues related to the communication between RT and the repository backend service, as well as fixing a race condition bug, which could result in the package signing process to fail when multiple requests were submitted at the same time.

7.4.2 Summary of service enhancements

Enhancements to the repository service include support for a new major release of the UMD repository, v5.0, by preparing the backend system and building the new release definition files for RPM-based systems. As part of the new major release, support for CentOS 8 systems was also introduced, which required compatibility changes due to the move from YUM to DNF in CentOS 8, as DNF does not support certain plugin-based YUM functionalities related to repository/package priority selection.

7.4.3 Future plans

Future plans for the EGI Software repository, apart from the regular maintenance tasks, include the integration with EGI AAI for authentication, instead of using the EGI SSO service and the possibility of providing a new frontend for the UMD and CMD repositories and moving away from RT in favor of another tool to handle requests.

7.5 Integration activities

During the last period, there was a shift in the authentication mechanisms used by the EGI Fedcloud infrastructure, as sites moved away from the traditional x509 VOMS method, in favour of OpenID connect authentication, using access tokens instead of proxy certificates. Due to this migration the AppDB needed to support the new authentication channels as well, in order to be able to deploy and manage VMs to the updated infrastructure endpoints via the VMOPs dashboard. As a result, a significant amount of effort went towards integrating related AppDB components with the EGI AAI OIDC Check-In service.

When a user tries to deploy a VM to an EGI Fedcloud endpoint via the VMOps dashboard, the system checks if this endpoint uses OIDC authentication; if so, it will check with the AppDB service whether an access token for the user already exists and is available. If not, the dashboard will prompt the user with a GUI dialog for consent to create a new access token to be used for the deployment. The dialog then redirects the user to the EGI AAI for credentials and if the user gets successfully authenticated, AAI transfers the user's access token to the AppDB service. From there, the VMOps dashboard may use this access token to proceed with deployment.

The same access token may be reused by the VMOps dashboard for other user activities until it expires, usually after an hour. If the user attempts to perform another action to the deployed VMs, AppDB will prompt the user again, in order to repeat the process of issuing a new access token from the EGI AAI.

8   Summary

The deliverable provides a detailed overview of the progress and achievements during the second reporting period of the project. It underlines the current status of integration work for all federation services included in the package, which has been being started according to the initial roadmap prepared during the first half of the project year and further evolved to address changing requirements of the stakeholders.

After establishment of the EOSC hub AAI architecture and initial integration of major AAI services a significant enhancement of the EOSC hub AAI in terms of aggregation and harmonisation of authorisation information (e.g. groups and/or roles) from multiple sources, adoption of standards and open technologies, including SAML 2.0, OpenID Connect, OAuth 2.0 and X.509v3 to facilitate interoperability and integration with the existing AAIs of e-Infrastructures and research communities has been accomplished.

The complexity and criticality of the distributed AAI architecture in terms of technology stack and compliance to the global policy frameworks like REFEDS and Sirtfi requires a modular approach in implementation and maintenance of AAI components by multiple groups of experts with specific expertise in their domains. This approach allows to break down the complexity and provides effective development of the EOSC hub AAI as a whole. The integration work is focused on technical alignment activities and policy-related integration activities. It has to be mentioned that although significant progress in the integration work, not all issues and integration gaps identified during the course of the project have been fully resolved so far, as some of them like reported "Multiple user registrations" or "Token validation" require changes in the protocol specifications and policy alignment by different e-infrastructures. The chosen strategy in WP5 to address these challenges is to provide workarounds to meet the requirements to AAI by other services and to develop a sustainable long-term solution to be implemented in the project lifetime.

The EOSC Hub Order Management System, which relies on several central components including Service Catalogue, Marketplace, Service Order Management Back Office (SOMBO) and integrates many other systems to facilitate promotion, discovery, access and ordering of the productional EOSC Hub services is another example of complex system, which provides core functions for the EOSC. A significant enhancement achieved during the second year of the project for this system is the successfully accomplished integration of Marketplace with SOMBO, which has been successfully deployed in production and ready for management of the order requests submitted in the Marketplace.

We faced the fact the further integration of core components of Order Management System with other order management systems of service providers will be quite complex and is not scalable according to the current design and integration scenarios, which assume the presence of advanced OMS by the service providers. The current observations show that most of the service providers and scientific communities don't have any mature management system to process the orders and often implement the order management via helpdesk systems. To address and mitigate this gap the WP5 and Marketplace developers are working on the White Label Marketplace, which can be provided for any service provider, who would like to be integrated with the EOSC Marketplace still keeping full control on the management of service orders. This solution also implies scalable integration of

White Label Marketplaces with EOSC Marketplace. The changes in the design of the EOSC Order Management System following this approach will be described in the next deliverable.

Many enhancements and integrations have been done in the service monitoring area. Stable development is observed for ARGO Monitoring and messaging systems. The specifications prepared by the expert groups deliver the architectures of these services together with interoperability guidelines for integration with external services.

Further enhancements after initial integration of EGI and EUDAT accounting systems have been implemented for single accounting services and repositories. Still more effort is required for aggregation and presentation of accounting information to address the EOSC accounting needs including the integrated dashboards with statistics for the services and resource usage. These requirements will be analysed and a modified roadmap for the accounting system will be established and implemented in the next project period.

A detailed current roadmap for the third year of the project is provided in the next chapter.

9 Roadmap

9.1 Identification, Authentication, Authorisation and Attribute Management

The roadmap of technical and policy-related alignment activities, which have been identified across the EOSC-hub AAI services, is maintained in the project wiki [R49]. The wiki page also includes the roadmap of integration activities among B2ACCESS, Check-in, INDIGO IAM and eduTEAMS. The subsections that follow provide the roadmaps of service enhancements which are specific to each EOSC-hub AAI service.

9.1.1 B2ACCESS

- Update of underlying software stack [Q2 2020]
- Reducing/removing further steps in user login workflow between B2ACCESS and Check-in [Q2 2020]

9.1.2 Check-in

- Improve integration with Community AAIs, including B2ACCESS, INDIGO IAM and eduTEAMS. Improvements include:
  - Skipping verification of email address when users authenticate with a verified email address [Q2 2020]
  - Simplifying IdP Discovery for end-users accessing services that support the AARC IdP-hinting specification AARC-G049 [R10] [Q4 2020]
- Add support for retrieving Proxy certificates through SSH key information managed by the EGI Check-in COmanage Registry [Q3 2020]
- Scope-based active attribute value selection: This enhancement will allow OAuth2 clients to limit the values of specific claims based on the requested scopes [Q2 2020]
- Improve the identity linking user experience and interface [Q3 2020]
  - Improve linked identities panel by including localised friendly name & logo of user's IdP
  - Enable implicit identity linking

9.1.3 eduTEAMS

- Include Monitoring and Alerting as a Service option to the eduTEAMS Dedicated and Bespoke offering [Q2 2020]
- New improved Discovery Service [Q2 2020]
- New improved MDQ Service [Q2 2020]
- Enhanced Community Attribute Profile support [Q2 2020]
- Improved support managing access to services per VO [Q2 2020]
- Support for AARC-G021 "Exchange of specific assurance information between Infrastructures" [Q3 2020]

- Support for AARC-G031 "Guidelines for evaluating the combined assurance of linked identities" [Q3 2020]
- Support for the updated version of AARC-G049 "A specification for IdP hinting" [Q3 2020]
- New OIDC frontend [Q3 2020]
- Improved IdP Registration flow [Q3 2020]
- Improved SP Management capabilities [Q4 2020]

9.1.4 INDIGO IAM

- Leverage Keycloak as the main IAM authentication engine. Keycloak is a flexible and popular open source solution by Redhat for centralized authentication and authorization. Integrating Keycloak in IAM will provide enhanced capabilities and improved sustainability [Q4 2020]

9.1.5 Perun

- New GUI [Q2 2020]
- Improved UX for the account linking [Q3 2020]
- Redesign workflow for account linking [Q3 2020]
- Performance optimization [Q4 2020]
- New user profile interface [Q3 2020]
- Improved integration with authentication proxies [Q4 2020]
- Improved user documentation [Q3 2020]
- Automatization of operation process [Q4 2020]
- New roles and authorization module [Q2 2020]
- Improved process for the synchronization of users, attributes and group from external systems [Q3 2020]

9.1.6 WaTTS

- Add fault tolerance, so that operation will not be interrupted, if once instance goes down [Q2 2020]

9.1.7 MasterPortal

- Support high availability deployment [Q3 2020]

9.1.8 RCauth - Online CA

- Support high availability deployment to allow distributing the service geographically across the federated operators, i.e. GRNET, STFC, and Nikhef [Q3 2020]

9.2 Marketplace and Order Management Tools

9.2.1 Marketplace

- Implementation of the helpdesk interface in Marketplace as a communication channel for general support of federated services [Q1 2020] -DONE
- Preparation of White Label solution of the Marketplace (content and graphical customizability) [Q2 2020]
- Enhancements in service offer attributes - structured schema, relational architecture reflected in filtering and search capabilities [Q3 2020]
- Analysis and implementation of OCRE use cases and requirements (accounting, ordering, vouchers) [Q4 2020]

9.2.2 Service Portfolio Management Tool

- Adapt service model to support SDT v2.10
  - Design & implement the Organisation Description Model from SDT v2.10 [Q3 2020]
  - Design & Implement the Service Description Model from SDT v2.10 [Q3 2020]
  - Design & Implement the relationship between Services & Organisations [Q3 2020]
  - Design & Implement the relationship between Organisations & Possible communication methods (API, e-mail etc). [Q3 2020]

9.3 Integrated Business and Operations Support Systems

9.3.1 Operations Portal

- Integration with EOSC AAI [Q2, 2020] - some attributes are still missing in the EOSC AAI system. Waiting for a fix.
- SLA Management Module in SOMBO [Q3, 2020]
  - For a given service order generate a document (or several documents) which will correspond to an agreement between the resource provider(s) and the customer.
  - The interface will provide different templates of documents depending on the type of resources.
- Add usage reports into the Service Order Management Back Office. [Q3,2020]
- Metrics module for EC [Q4,2020] - Partially released in April

9.3.2 GOCDB

- Improve configuration management to ensure the long-term stability of the service [Q2,2020]
- Improvements and modification of "Reserved Scopes" handling in GOCDB [Q2,2020]
- Creating new EOSC-Hub specific ServiceTypes automatically when they are added to the EOSC-Hub SPMT API. [Q2,2020]
- A second, configuration managed, production instance of GOCDB will be deployed behind our load balancer. [Q2,2020]

- The functionality of the Write API will be expanded to meet evolving use cases. [Q2,2020]
- EOSC-hub separate view under its own URL to show resources with the 'EOSC-Hub' scope tag applied, and we will use the current ServiceGroup functionality to represent EOSC-Hub's federated services. [Q1,2020]

9.3.3 Data Project Management Tool

- Migration to Plone 5.2 and Python 3 [Q2,2020]
- Connect DPMTs request handling to the EOSC order management via a message bus to be in line with the general switch to the AMS message bus for communication between services [Q2,2020]
- When collecting service information from SPMT: switch to SPMT API version 2 [Q2,2020]

9.3.4 Data Management Planning Tool

- Align the schema of EasyDMP with that of the RDA common DMP standard to demonstrate the interoperability between EasyDMP and openDMP by exporting plan from one tool to another. [Q2, 2020] - IN PROGRESS
- Further services that make the data management plans machine actionable and verifiable will be developed as part of EOSC-HUB and interfaced to easyDMP and openDMP. [2020] - ONGOING
- Support local deployments of the eestore and extend the resources harvested (to include the SPMT/DPMT). [Q2,2020] DONE
- To onboard the OpenDMP tool into the EOSC portfolio of services. [Q1,2020] - DONE
    - This is part of the openAIRE framework
- Integration with DMPT and automatic procedure for update of data management plan based on the information provided in Marketplace order. [Q3, 2020] -IN PROGRESS

9.3.5 SVMON

- Distribution of the SVMON client among service providers [2020]
- Implementation of token-based authentication for reporting agents [Q1,2020] - DONE

9.4 Monitoring, Accounting, Messaging, Security Tools

9.4.1 Accounting Repository

- Fixes to SLUM parser [Q1,2020]
- New interface and API for publishing and synchronisation tests [Q2,2020]
- Summary storage accounting record format to produce consistent aggregations to reduce the volume of data to transfer [Q2,2020]
- Improvement of AMS integration including making certificates optional [Q3,2020]
- Enhancements to storage accounting [Q3,2020]
- Support of DODAS thematic service for deployment of accounting probes to report usage metrics from automatically deployed clusters [Q2,2020]

9.4.2 **Accounting Portal**

- Move Storage accounting to production after APEL update [Q1, 2020]
- Improve WLCG dedicated sections in Accounting Portal [Q1, 2020]
- Transition from AMS to SSM [Q2, 2020]
- Further Improvement of EUDAT dedicated sections in Accounting Portal [Q2, 2020]

9.4.3 **ARGO Monitoring**

- **Harmonization of the user facing web interface**: The new versions of the ARGO A/R and Status web interface and the POEM web interface will soon have similar look and feel [Q1,2020]
- **Single stop shop for service enablement and configuration**: This activity is designing a service management web interface through which customers (e.g. VO managers, Infrastructure Managers etc) will be able to configure the monitoring service to their liking. [Q3, 2020]
- **Customer defined thresholds**: This activity will allow ARGO customers (e.g. VO managers, Infrastructure Managers etc) to set multiple threshold profiles for each individual metric or specific service endpoint to generate reports. [Q2,2020]

9.4.4 **ARGO Messaging Service**

- Support, maintain, extend the AMS Service [2020]
- Support, maintain, extend the AuhN Service [2020]
- Support FedCloud information System [2020]
- Support EGI Information System [2020]
- Support AppDB [2020]

9.4.5 **Security Tools**

9.4.5.1 *Pakiti*

- Evaluation of new Pakiti service version [Q1,2020]
- Support and maintenance [2020]

9.4.5.2 *Secant*

- OpenStack support [2020]
- Integration with AppDB [Q3,2020]

9.5 Helpdesk Services and Tools

9.5.1 **GGUS**

- Regular bi-monthly release schedule, security updates, implementation requested features [2020]

9.5.2 **EUDAT-RT**

- Maintenance and regular updates, no further development or integration is planned [2020]

9.5.3 **xGUS**

- Integration with multiple web interfaces for request submission provided by EOSC portal, Marketplace [Q1, 2020]-DONE
- Maintenance and security patches [2020]

9.6 Application store, Software Repositories

9.6.1 **Application Database**

- Replaced ldap queries to top-BDII's with the AMS (Argo Messaging Service) message queue as a transport mechanism, in order to retrieve latest infrastructure (cloud) information [Q1,2020] - DONE (in dev instance)
- Provide support for OpenID Connect [Q1, 2020] - DONE (in dev instance)
- Extend the AppDB IS to support GLUE 2.1 schema [Q1, 2020] - DONE (in dev instance)
- Provide support for native APIs in VMOps dashboards [Q2, 2020]
- Drop OCCI support from VMOps dashboard [Q2, 2020]
- Development of the Endorser Dashboard [Q3, 2020]
- Development of the Security Dashboard [Q4, 2020]

9.6.2 **GitLab**

- Support and maintenance of entire DevOps cycle [2020]
- Increase resources for the instance from 6GB to 16GB [Q2, 2020]

9.6.3 **EGI software repository**

- Move from EGI SSO to EGI AAI authentication for admin instance [Q3, 2020]
- Provide a new front-end for the UMD / CMD and internal production software repositories, based on the AppDB portal codebase. [Q4, 2020]
- Move from RT to some other system, such as JIRA or AMS, for the software provisioning process. [Q4, 2020]

10 References

No	Description/Link
R1	https://aarc-community.org/
R2	https://refeds.org/category/research-and-scholarship
R3	https://refeds.org/sirtfi
R4	https://refeds.org/assurance
R5	https://confluence.egi.eu/display/EOSC/AAI+Roadmap
R6	https://documents.egi.eu/public/ShowDocument?docid=3344
R7	https://documents.egi.eu/public/ShowDocument?docid=3561
R8	https://tools.ietf.org/html/rfc8628
R9	https://aarc-community.org/guidelines/aarc-g027/
R10	https://aarc-community.org/guidelines/aarc-g049
R11	https://aai.egi.eu/sshkeys
R12	https://aai.egi.eu/registry/
R13	https://documents.egi.eu/public/ShowDocument?docid=3503
R14	https://aws.amazon.com/contract-center/geant/
R15	https://semver.org/
R16	https://www.eduteams.org/#offerings
R17	https://members.orcid.org/api
R18	http://erlang.org/doc/apps/mnesia/index.html
R19	https://www.cilogon.org/
R20	https://aarc-community.org/guidelines/aarc-g049/
R21	http://openid.net/specs/openid-connect-federation-1_0.html
R22	https://docs.google.com/document/d/11Amv6kjPvVVgWB71iEaj6NcrhlNzht7HP9GJK6cNOS8/edit
R23	https://tools.ietf.org/html/rfc7662
R24	https://refeds.org/category/research-and-scholarship
R25	https://aarc-community.org/guidelines/aarc-g002/
R26	https://aarc-community.org/guidelines/aarc-g027/
R27	https://aarc-community.org/guidelines/aarc-g025/

R28	https://wiki.refeds.org/display/ASS/REFEDS+Assurance+Framework+ver+1.0
R29	https://aarc-community.org/guidelines/aarc-g021/
R30	https://aarc-community.org/guidelines/aarc-g031/
R31	https://aarc-community.org/guidelines/aarc-g041/
R32	https://aarc-community.org/guidelines/aarc-g025/
R33	https://docs.google.com/document/d/11Amv6kjPvVVgWB71iEaj6NcrhlNzht7HP9GJK6cNOS8/edit
R34	http://openid.net/specs/openid-connect-federation-1_0.html
R35	https://wiki.refeds.org/download/attachments/1606087/GEANT_DP_CoCo_ver1.0.pdf?version=1&modificationDate=1450367740260&api=v2
R36	https://aarc-community.org/guidelines/aarc-g040/
R37	https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf
R38	https://wiki.geant.org/download/attachments/123766285/WISE-SCI-Baseline-AUP-V1.0.1-draft.pdf?version=1&modificationDate=1557297275149&api=v2
R39	https://fitsm.itemo.org/
R40	https://opendmp.eu/home
R41	https://eosc.ui.devel.argo.grnet.gr
R42	https://getpostman.com
R43	https://www.getpostman.com/docs/collections
R44	https://api-doc.argo.grnet.gr/argo-messaging/
R45	https://cloud.google.com/pubsub/docs/release-notes
R46	https://wiki.egi.eu/wiki/GGUS
R47	https://wiki.egi.eu/wiki/GGUS:Main_Page
R48	https://ggus.eu/index.php?mode=release_notes
R49	https://confluence.egi.eu/display/EOSC/AAI+Roadmap
R50	https://tools.ietf.org/html/rfc8628
R51	https://doi.org/10.5281/zenodo.3672784
R52	https://zenodo.org/record/1308682#.Xti-U_lS9hF