EOSC-hub

D5.2 First release of federation and collaboration services and tools

Lead Partner:	GRNET
Version:	1.0
Status:	Final
Dissemination Level:	Public
Document Link:	https://documents.egi.eu/document/3418

Deliverable Abstract

This document provides an overview of the EOSC-hub federation and collaboration services and tools and describes corrections, changes or enhancements made during the first year of the project. These changes have been implemented according to the initial integration plans and the evolving requirements from the user communities. The release notes included in the document are classified into different categories and are presented in a uniform format. An outline of the future plans is also provided for each WP5 service/tool.

OSC-HUB RECEIVES FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER
RANT AGREEMENT NO. 777536.

COPYRIGHT NOTICE

DELIVERY SLIP

Date	*Name*	*Partner/Activity*	*Date*
From:	Nicolas Liampotis	GRNET/WP5	2018-12-31
Moderated by:	Małgorzata Krakowian	EGI Foundation/WP1	
Reviewed by:	Alessandro Paolini Enol Fernández	EGI Foundation/WP4 EGI Foundation/WP6	2019-01-11
Approved by:	AMB		

DOCUMENT LOG

Issue	*Date*	*Comment*	*Author*
v.0.1	2018-10-24	Finalised table of contents	Nicolas Liampotis, Pavel Weber
v.0.2	2018-11-01	Added Content for ARGO Monitoring / Messaging, AGORA/SPMT	Themis Zamani, Kostas Koumantaros
v.0.3	2018-11-22	All contributions for sections/tools provided	WP5 service/tool owners
v.0.4	2018-12-22	Added executive summary	Nicolas Liampotis
v.0.5	2018-12-30	Added glossary	Nicolas Liampotis
v.0.6	2018-12-31	Ready for external review	Nicolas Liampotis
v.0.7	2019-01-11	Comments added by external reviewers	Alessandro Paolini, Enol Fernández
v.1.0	2019-01-18	Final version	Nicolas Liampotis

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
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
LB	Load Balancing
OIDC	OpenID Connect
OLA	Operational Level Agreement
PKIX	Public-Key Infrastructure (X.509)
SLA	Service Level Agreement
PID	Persistent Identifier
SP	Service Provider
SAML	Security Assertion Markup Language
VM	Virtual Machine
VO	Virtual Organisation
VOMS	Virtual Organization Membership Service

Contents

Executive summary

The focus of Work Package 5 (WP5) is on the federation and collaboration services and tools. WP5 aims to seamlessly integrate these services and tools and support their interoperability to create a framework that will enable the service federation in the EOSC, including common (WP6) and thematic services (WP7). WP5 maintains the high-quality of the federation and collaboration services and tools according to a maintenance plan, and ensures that they evolve according to the developing requirements coming from the user communities. This document provides an overview of these federation and collaboration services and tools and describes corrections, changes or enhancements made during the first year of the project.

The EOSC-hub Authentication and Authorization Infrastructure (AAI) task aims to contribute to the EOSC infrastructure implementation roadmap by enabling seamless access to a system of research data and services. The EOSC-hub AAI builds on existing AAI solutions from the EGI Federation, EUDAT CDI, INDIGO-DataCloud and GEANT. During the first year of the project, the AAI task put the focus on the initial integration required for demonstrating technical ability for communities using either **B2ACCESS** or **Check-in** for their community AAI to use services behind the EGI and EUDAT e-Infrastructure SP Proxies. Specifically, a researcher whose community is managed by B2ACCESS should be able to access EGI services. Likewise, a researcher whose community is managed by Check-in should be able to access EUDAT services. The task's future plans include the improvement of this initial integration between Check-in and B2ACCESS as well as the interconnection of all EOSC-hub AAI services, i.e. **GEANT eduTEAMS** and **INDIGO IAM**, and the finalisation of the remaining harmonisation activities on the technical and policy level (e.g. alignment of Acceptable Use Policies). **Perun** is an Identity and Access Management system used in EOSC-hub for managing users within organisations and projects, as well as managing access rights to the services. During the first year of the project Perun was added an option for the Membership Management Service of eduTEAMS, while a number of new features and improvements, as well as bug fixes were provided. Future plans include tighter integration with Check-in, a new graphical user interface and improvements in the user experience for account linking. Service capability alignment between **WaTTS** and **MasterPortal** is ongoing, and although at this point the two token translation services provide slightly different capabilities and a different focus, it is feasible that both tools evolve in a way that allows merging of the services. Regarding the **RCauth.eu Online CA** service, it is necessary to distribute the service geographically and move to a full active-active redundant set-up across different operators, i.e. Nikhef, GRNET and STFC.

The EOSC-hub **Marketplace (MP)** is a user-facing platform where production EOSC-hub services can be promoted, discovered, ordered and accessed. During the first months of the EOSC-hub project, the look and feel of the MP Platform was adapted to the EOSC-hub environment and a separate installation was instantiated, ready to be populated with EOSC-hub providers and services. The decision to use the EOSC-hub Marketplace as the EOSC Marketplace led to a deep analysis of the platform which resulted in rewriting the existing solution and extending it with functionalities required for EOSC. The next steps will rely on the feedback following the launch of the EOSC Portal. The **Service Portfolio Management Tool (SPMT/AGORA)** allows managing service descriptions according to the service management guidelines of FitSM. The SPMT also allows

exporting service descriptions to other tools and service catalogues, such as the EOSC-hub service catalogue [R1]. Apart from a number of enhancements that have been agreed to suit the needs and requirements of the EOSC-hub communities, it is also foreseen to continue working on the integration between the SPMT and the Marketplace, as well as with other operational services, such as the GOCDB and the DPMT (see below), that will allow the Marketplace to automatically retrieve and publish information about the services.

WP5 also includes a suite of services that facilitate the EOSC-hub operations, configuration and change management, as well as distributed order management processes. The **Operations Portal** is a central platform for the operations community that offers a bundle of different capabilities, such as the broadcast tool, Virtual Organization (VO) management facilities, a security dashboard and an operations dashboard that is used to display information about failing monitoring probes and to open tickets against underperforming Resource Centres. During the first 12 months, the **GOCDB** introduced new features, most notably the 'notify' feature that allows users to receive notifications about Sites and Services. This 'notify' feature is used by the ARGO notifications component to inform (or not) the Sites and Services owners about important events (when critical infrastructure components fail and recover). Future plans include extending the write API and adding an EOSC-specific view to represent EOSC's topology. To ensure the long-term stability of the service, the configuration management of the GOCDB will be improved. The **Data Project Management Tool (DPMT)** is used by the EUDAT CDI to coordinate the engagement and contributions of the various partners of the distributed data infrastructure. In order to integrate this service into the developing EOSC ecosystem several steps have been taken, including the extension of DPMT's compatibility layer with the GOCDB. This facilitates the integration of information from the GOCDB and it also allows third parties to interact with the DPMT and the GOCDB in a uniform way. In addition, DPMT can now expose information about resource consumption for accounting purposes in StAR format as proposed by the Open Grid Forum (OGF) and planned to be consumed by EOSC's forthcoming accounting system. The **Data Management Planning Tool (EasyDMP)** is a tool for creating machine-actionable data management plans that can then be used by data management services to enforce the plan. During the first year of the project, the external entity registry service (eestore) for the user-interface of the EasyDMP tool was developed. It should be noted that the work on the tool for data management plans is also carried out in collaboration with OpenAIRE-Advance. The OpenAIRE-Advance/EOSC-hub tool is called openDMP. Further services that make the data management plans machine actionable and verifiable will be developed and integrated with both easyDMP and openDMP. The **SVMON** and **Pakiti** systems provide the possibility to monitor the software versions installed at data centres participating in the EOSC-hub project. The focus of the Pakiti system is security monitoring, while the SVMON facilitates release and deployment management. As both tools have much in common and provide complementary functionality on the client side, it was decided to integrate their clients. The initial integration of SVMON client with Pakiti client is already accomplished, which allows running SVMON client as a module connected to Pakiti client. This approach unifies the installation of SVMON client together with Pakiti and allows service owners to choose between one or both clients. The Pakiti server has been operated and maintained according to the needs of EGI CSIRT and other security teams. There has been significant progress with the implementation of the new Pakiti server and its evaluation through pilot operations. The new version of the server will be deployed in 2019. It will be operated and maintained according to the needs of the EOSC-hub security teams.

The **Accounting Repository** 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 available through the **Accounting Portal**. Apart from working on the integration of EGI and EUDAT accounting services, the accounting team is planning to switch from the old Message Brokers Network to the new Argo Messaging service (see below) as its transport mechanism. **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. The monitoring systems based on ARGO framework are already successfully used by both EGI and EUDAT infrastructures. Thus, the work during the first year of the project put the focus on the development of a web-portal providing a unified EOSC-hub view on monitoring information. Future plans include the harmonisation of all user-facing web interfaces, the provision of a single stop shop for service enablement and configuration, as well as the support for customer-defined thresholds. The **ARGO Messaging Service (AMS)** enables reliable asynchronous messaging for the EOSC-hub infrastructure. It provides an HTTP API that enables Users/Systems to implement a message-oriented service using the Publish/Subscribe Model. In the current deployment a haproxy server acts as load balancer for the 3 AMS servers running in the backend. A notable enhancement of the service during the first year of the project was adding support for translating x509 certificates to AMS tokens to allow/ease the onboarding of the remainder users of the old Message Broker Network to the new AMS Service. **Secant** is a cloud security assessment framework which has been significantly reworked with a number of improvements to enhance the utility and robustness. The changes are related to the controlling of virtual machines, log management, stability, and change configuration. The set of security probes was reviewed and new probes were added, e.g. to check ssh passwords and exposed vulnerabilities. Secant has been integrated with the AppDB so that new virtual appliances can be checked during the registration process. Future developments will focus on other aspects related to the integration with the AppDB (see below).

There are two systems that have been used in production for incident and service request management, as well as problem management processes: **GGUS** for EGI and **Request Tracker (RT)** for EUDAT. During the first year of the project, **xGUS** was developed in order to provide a unique entry point to these two ticketing systems. xGUS is directly integrated with the GGUS system and also provides an API to allow integration with RT. This new solution is already used in production for managing first level support tickets, as well as for escalating and categorising any request or problem submitted. Future plans include the improvement of the current integration with RT and other enhancements based on the requirements from the user support team.

The **Applications Database (AppDB)** is a central service that maintains information about software solutions and virtual appliances (VAs). In addition, AppDB is responsible for distributing the registered VM images to the resource providers and enabling users to deploy and manage Virtual Machines to the EGI Cloud infrastructure. During the first year of the project several new features were introduced along with improvements to existing features and the regular bug fixes.

Integration with the Secant tool using the EGI Argo Messaging Service allowed for automated security checks for all VA versions upon publishing, as well as visual feedback of security checks for each VA version in VO image lists. AppDB's platform also got extended with support for persistent identifiers (PIDs) for registered digital objects (software & Virtual Appliances) through the use of open standards, such as the HANDLE system. In the context of collaboration with OpenAIRE-Advance, a new OAI-PMH server interface was developed to expose the metadata of registered products to the OpenAIRE harvesting services. Future plans include adding support for OpenID Connect and extending the AppDB Information Service (IS) to support GLUE 2.1 schema. As for the AppDB VM Operations (VMOps) service, certain improvements to the existing operations dashboard are foreseen, as well as developing a new dashboard accessible by a special group of experts, through which they will be able to endorse or un-endorse VMs (VA versions) registered with the AppDB system. **GitLab** is a web-based platform which provides an integrated environment for software development including Git-repository, issue tracking system, wiki, continuous integration module etc. GitLab is used in EOSC-hub as an integrated solution for software development, as well as for automating workflows for release and deployment management. The EOSC-hub GitLab instance has enabled federated access and has been integrated with Container Registry for allowing storing Docker images. Future plans include the deployment of GitLab runners to accelerate the build, test, deployment, and monitoring process for software projects. It is also foreseen to integrate GitLab as a software repository for the AppDB. The **EGI Software Repository** is a collection of services for supporting the management and the provisioning of the software artefacts that compose the Unified Middleware Distribution (UMD) and the Cloud Middleware Distribution (CMD), the Community Repositories, and the operational tools developed by the consortium. Work on employing Jenkins as a platform tool for Continuous Integration (CI) with respect to UMD is already in progress. Furthermore, the idea of using the AppDB portal as the front-end for the EGI software repository is under evaluation.

1 Introduction

This document provides an overview of the EOSC-hub federation and collaboration services and tools and describes all notable corrections, changes or enhancements made during the first year of the project. These changes have been prepared and agreed among the WP5 partners and are the result of the implementation of the initial integration plans presented in “D5.1 Initial maintenance and integration plan for federation and collaboration services”.

The description of the federation and collaboration services and tools and related release notes and future plans is grouped into 6 major chapters following the structure of WP5 which is itself organised in 6 tasks. Each chapter provides an overview of the services and tools included in the corresponding task to help better understand the structure and logical as well as technical setup. The task overview section is followed by sections dedicated to the services/tools under that task. These sections provide an overview of the described service/tool along with the release notes and future plans.

Changes listed in the release notes sections have been classified as follows:

- *Added* - for new features.
- *Changed* - for changes in existing functionality.
- *Deprecated* - for soon-to-be removed features.
- *Removed* - for now removed features.
- *Fixed* - for any bug fixes.
- *Security* - in case of vulnerabilities.

Where possible, the release notes follow the presentation format documented in [R2].

2 Identification, Authentication, Authorisation and Attribute Management

2.1 Overview

This chapter presents the release notes and future plans for the AAI services that enable seamless access to research data and services in EOSC-hub. Solutions from EGI, EUDAT, GÉANT and INDIGO that have successfully delivered a portfolio of operational services (Technology Readiness Levels above TRL 7) in this field over the last years are the initial basis of the integrated EOSC-hub AAI. These AAI solutions, namely B2ACCESS, Check-in, eduTEAMS and INDIGO-IAM connect to eduGAIN as service providers but act as identity providers from the services point of view, thereby allowing users to use their credentials from their home organisations. Compliance with policy frameworks such as the REFEDS Research and Scholarship entity category and Sirtfi, facilitates sufficient attribute release, as well as operational security, incident response, and traceability. Complementary to this, users without an account on a federated institutional Identity Provider are still able to use social media or other external authentication providers for accessing services. Thus, access can be expanded outside the traditional user base, opening services to all user groups including researchers, people in higher-education, and members of business organisations. Research communities can leverage the EOSC-hub AAI services for managing their users and their respective roles and other authorisation-related information. At the same time, the adoption of standards and open technologies, including SAML 2.0, OpenID Connect, OAuth 2.0 and X.509v3, facilitates interoperability and integration with the existing AAIs of other e-Infrastructures and research communities.

The suite of EOSC-hub AAI services also includes Perun, which can be used 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 on-the-fly identify entities based on federated credentials and issue to them PKIX credentials in real-time, focussing on converting SAML-to-PKIX.

2.2 B2ACCESS

2.2.1 Overview

Service/Tool name	B2ACCESS
Service/Tool url	https://b2access.eudat.eu
Service/Tool information page	https://www.eudat.eu/services/b2access
Description	The B2ACCESS service is an Identity and Access Management (IAM) system which arbitrates authenticated access to registered services. The role of the B2ACCESS service is to allow these services to perform authentication,

	to take authorisation decisions, and to perform any other processing of user information (e.g. harmonisation or translation), when end users access these services.
Value proposition	B2ACCESS acts as a proxy IdP, following the AARC Blueprint Architecture, which allows users to sign in with their preferred primary identities. These identities can be provided by external identity providers, e.g. Shibboleth IdPs of the users' home organisations or OpenID Connect providers such as the Google IdP, or they can be provided by the B2ACCESS service itself, if the users registered genuinely on this service. B2ACCESS supports multiple protocols for authentication, such as SAML and OpenID Connect/OAuth2, for external identity and service providers. It translates the attributes from one protocol to another. This, for instance, allows users of a service, connected via the OAuth2 protocol, to sign in with their home organisation identity provider, connected via SAML. Besides identity management, B2ACCESS provides group and attribute management, too. Accounts can be extended by attributes, which are needed by connected services, but not provided by the external identity provider, e.g. assurance information. Hierarchical groups allow for flexible group management, e.g. separations by resources or thematic diversity. Both features offer the possibility for fine grained authorisation decisions. The attribute, identity and group management can be done by the web interface or the REST API.
Customer of the service/tool	Resource Provider; Research Communities
User of the service/tool	Community/VO managers, researchers, Operations Managers for research infrastructures/collaborations
User Documentation	https://eudat.eu/services/userdoc/b2access-management
Technical Documentation	Service integration: https://eudat.eu/services/userdoc/b2access-service-integration Unity manual: http://www.unity-idm.eu/documentation/unity-2.4.2/manual.html
Product team	JUELICH
License	http://www.unity-idm.eu/opensource/[1]
Source code	Unity: https://github.com/unity-idm/unity EUDAT extension: https://github.com/EUDAT-B2ACCESS/b2access-unitytheme
Testing	Each new release of the underlying software must pass a set of tests. These tests are conducted in two steps. First, the basic functionality of the software itself is tested. There is no integration with external authentication services and only demonstration services are connected as service providers. In the second step, the software is tested in an environment closely resembling to the production system. In addition to the test of the specific operating system level, the integration of external authentication services like eduGAIN or Google is tested. All tests are done by operators,

[1] The Unity-IDM license complies with the Open Source Definition since redistribution and use in source and binary forms, with or without modification, are permitted provided that the conditions listed in http://www.unity-idm.eu/opensource/ are met.

	who know the service, and users who do not know the setup. If some tests fail, the problem is investigated. If there is no solution to pass the test, e.g. because of a bug inside the software, the version is skipped.

2.2.2 Release notes

2018-09

Changed

- Replace cn as required attribute by givenName and sn.

2018-04

Added

- Included Check-in as IdP and SP.
- Release group membership information according to AARC guidelines AARC-G002 [R3].

2.2.3 Future plans

- New UI at login screen.
- Reducing/removing steps in user login workflow between B2ACCESS and Check-in.

2.3 Check-in

2.3.1 Overview

Service/Tool name	EGI Check-in
Service/Tool url	https://aai.egi.eu/
Service/Tool information page	https://wiki.egi.eu/wiki/AAI
Description	The EGI Check-in service is an Identity and Access Management solution that makes it easy to secure access to services and resources.
Value proposition	Through Check-in, users are able to authenticate with the credentials provided by the IdP of their Home Organisation (e.g. via eduGAIN), as well as using social identity providers, or other selected external identity providers. Check-in provides an intuitive interface for communities to manage their users and their respective groups, roles and access rights. For communities operating their own group management system, Check-in has a comprehensive list of connectors that allows to integrate their systems as externally managed Attribute Authorities.
Customer of the service/tool	Research Infrastructures, Research Communities, Resource Providers

User of the service/tool	Community/VO managers, researchers, Operations Managers for research infrastructures/collaborations
User Documentation	https://wiki.egi.eu/wiki/AAI#Documentation
Technical Documentation	https://wiki.egi.eu/wiki/AAI#Documentation
Product team	GRNET
License	Apache License Version 2.0
Source code	https://github.com/rciam https://github.com/EGI-Foundation/simplesamlphp-module-themeegi
Testing	Functional and user interface testing is being held before every change. Higher risk changes are reviewed by the EGI Change Advisory Board before being released in production.

2.3.2 Release notes

v18.10.1 - 2018-10-30

Added

- Add banner and an extra view for cookie options
- Add corner ribbon that displays customisable text
- Module discopower: Add style rules and logos for the IdPs (eduTEAMS, EGI SSO, Aria)

Changed

- Update footer style

v18.04.2 - 2018-04-17

Added

- Create new theme for SimpleSAMLphp based on Bootstrap.

v18.04.1 - 2018-04-11

Added

- Integrate B2ACCESS as IdP and SP.

v18.03.1 - 2018-03-01

Removed

- Disable dynamic OpenID Connect/OAuth2 client registration via /register endpoint.

v18.02.2 - 2018-02-23

Added

- Add “Approved Services” page to allow users view and revoke active access/refresh tokens that have been issued for OpenID Connect/OAuth2 clients.
- Add support for configuring default and max validity time of tokens. Don’t allow refresh tokens that never expire

- Add support for single logout.

Changed

- Add iss(issuer) claim in token introspection response. The value of the claim is obtained dynamically.

Fixed

- UTF8 encoding bug in MySQL

v18.02.1 - 2018-02-22

Changed

- Release group membership information according to AARC guidelines AARC-G002 [R3].

Unreleased (changes under testing/piloting in development instance)

Added

- Add support for VOMS (de)provisioning of users
- Add support for OAuth 2.0 token exchange according to draft specification.
- Add support for configuring naming of claims.
- Add cookie policy and cookie banner.
- Add admin role based on entitlement and/or sub. Give admin privileges to users that contain a certain entitlement and\or sub.

Changed

- Add non-standard OAuth2 scopes for requesting eduPerson related claims
- Allow dynamic client registration for token-exchange. Users can register a client with token-exchange as grant type.
- Change default/restricted system scopes.
- Move all configuration options to application.oidc.properties file.
- Update EGI Check-in theme.

Fixed

- Don't allow token response if client has no scopes defined.

2.3.3 Future plans

- Improve integration with EUDAT B2ACCESS
- Integrate with eduTEAMS to enable communities managed by eduTEAMS to access EGI services and resources
- Integrate with INDIGO-IAM to enable communities managed by INDIGO-IAM to access EGI services and resources
- Improve integration with Perun
- Provide uniform look and feel across all Check-in service component UIs
- Add support for (de-)provisioning and continuous update of user account information:
  - VOMS (COmanage plugin currently being tested in the development environment)
  - SCIM

2.4 eduTEAMS

2.4.1 Overview

Service/Tool name	eduTEAMS
Service/Tool url	http://www.eduteams.org
Service/Tool information page	https://wiki.geant.org/display/eduTEAMS
Description	eduTEAMS enables researchers, students and other members of the research and education community to create and manage virtual teams and securely access and share common resources and services using federated identities from eduGAIN and trusted Identity Providers.
Value proposition	The eduTEAMS service enables research communities to securely access and share common resources and services. Leveraging the ubiquitous presence of eduGAIN federated identities, eduTEAMS enables communities to securely authenticate and identify their users, organize them in groups, assign them roles and centrally manage access rights for using community resources. As research is not confined only in the research institutes and universities, eduTEAMS caters also for users coming from the industry or citizen scientists who may not have access to eduGAIN. It does so by supporting external (non-eduGAIN) identity providers, such as social networks providing federated identities, community identity providers and other platforms that can provided federated user identities. Communities can use the eduTEAMS service as the community AAI for their virtual collaborations.
Customer of the service/tool	Research Infrastructures, Research Communities
User of the service/tool	Community/VO managers, researchers, students, faculty of academic institutions, IT support staff for RIs/RCs
User Documentation	https://wiki.geant.org/display/eduTEAMS
Technical Documentation	https://wiki.geant.org/display/eduTEAMS
Product team	GÉANT
License	Not applicable
Source code	eduTEAMS is based on open source software: https://github.com/IdentityPython/ https://spaces.at.internet2.edu/display/COmanage/Home

	https://github.com/hexaaproject https://github.com/CESNET/perun https://github.com/CESNET/perun-services https://github.com/CESNET/perun-wui
Testing	The GÉANT Service Quality Assurance team provides QA testing to the GÉANT service. The QA involves: • Quality code audit - automatic code review completed by the code inspection (expert analysis) to examine the source code and identify: potential bugs, bad code architecture, duplicated code and similar coding irregularities. • Security code audit - automatic code review completed by the code inspection (expert analysis) to examine the source code and identify the largest possible number of source code security flaws and vulnerabilities. • Vulnerability assessment (aka security testing) - a thorough process of system security testing from a user's as well as inside and outside (black-box) point of view together with testing of the underlying operating system, other software package dependencies and its configurations. • Documentation evaluation - usually the first sanity check aiming to help to identify early potential risks (ie. the required documentation is missing), spaces for improvements and possibilities for optimizing the system (ie. desirable documentation is missing). • Operational testing - in-depth review of the operational documentation against the completeness, correctness and comprehensiveness. Someone not familiar with the service will try to reproduce all steps listed in the documentation and verifies the outcome. • Functional and user interface testing - it is composed of the usability and accessibility testing mixed with some elements of functional tests of the user interface and the web user interface. • Performance testing - to measure how the system behaves in various predefined conditions, to check if the service meets the expected KPI and to identify potential bottlenecks.

2.4.2 Release notes

201810

Changed

- Updated privacy policy
- [Proxy] Improved support for informing the users about the attributes released to the connected services
- [Proxy] Improved backend integration with COmanage and HEXAA
- [MMS] Improved support for account linking
- [MMS] UI improvements for COmanage, HEXAA and Perun

201809

Changed

- [MMS] Improved registration flow for new VOs for COmanage, HEXAA and Perun

Deprecated

- [MMS] Self registration of VOs in the demo service will be removed in November. Users can still request new VOs on any of the supported MMSs and the applications will be reviewed by the eduTEAMS team
- [MMS] The separate demo service will be discontinued in December. The ability to demo the eduTEAMS will be incorporated in the eduTEAMS Service itself

201808

Changed

- All web user interfaces include a link to the eduTEAMS Privacy Policy

201807

Added

- Introduction of the eduTEAMS demo service
- [DS] Added support for HA and LB
- [MMS] Introduction of the Master MMS. User can now register on the eduTEAMS platform and create or join VOs on any of the supported MMS
- Introduction of the community registry service

201806

Added

- [MMS] HEXAA and Perun as options for the Membership Management Service in addition to COmanage
- [DS] New UI and visual identity based on the RA21 recommendation
- [DS] Improved search performance
- [Proxy] Support for VOPerson and VOPersonExternalAffiliation
- [Proxy] Support for injecting user attributes based on IdP and SP metadata
- [Proxy] New policy engine for static attributes
- [Proxy] Improved support for ORCID, Google and Facebook as external Identity Providers

201805

Changed

- [Proxy] Updated to the latest version of SATOSA
- [DS] Updated to the latest version of PyFF

201804

Added

- [Proxy] Configurable memoization of IdP selection when using MDQ

Changed

- [Proxy] Updated to the latest version of SATOSA
- [DS] Updated to the latest version of PyFF

2.4.3 Future plans

- eduTEAMS Dedicated and Bespoke Service Offering
- Step-up authentication service

2.5 Perun

2.5.1 Overview

Service/Tool name	Perun
Service/Tool url	https://perun.egi.eu/
Service/Tool information page	https://perun-aai.org/
Description	Perun is an Identity and Access management software that covers management of the whole ecosystem around the users' identities, groups, resources and services. Perun is well suited for managing users within organizations and projects, managing access rights to the services. Perun is designed to be flexible and customizable, therefore it can be easily integrated with other tools or incorporated into existing workflows. Moreover Perun stresses decentralization of authorization decisions by empowering end users to manage groups within it and delegate this privilege to other users.
Value proposition	Identity and Access management system that can be offered as stand alone tool or it can be integrated with other EOSC-hub components like authentication proxies and delivered as an integrated service offer. Perun supports advanced features and use-cases like self-service, privilege delegation, account linking, provisioning and deprovisioning or integration with CSIRT.
Customer of the service/tool	Research Communities, Research Infrastructures
User of the service/tool	Virtual Organization Managers, Services Managers, Virtual Organization members, Members of CSIRT
User Documentation	https://perun-aai.org/documentation/user-documentation
Technical Documentation	https://perun-aai.org/documentation/technical-documentation
Product team	CESNET
License	BSD 2-Clause
Source code	https://github.com/CESNET/perun https://github.com/CESNET/perun-services

	https://github.com/CESNET/perun-wui
Testing	Automatic unit and integration tests are part of development and deployment process. The code review is a part of the development process. Regular penetration testing every second year.

2.5.2 Release notes

2018-11-20

Added

- [CORE] Gather IdP and IdPs organzation name attributes.
- [CORE] Upgrade to Spring 5.1
- [CORE] Hide create VO button in GUI is configured for specific instance.
- [CORE] Auto-create member:def:organization attribute.
- [CORE] Check input length of user titles.
- [CORE] Perun admin can switch between types of users: sponsored, service and normal users.
- [CORE] Initial support for new ways of auditing (each message is an object, stored as simple json in new table).
- [CORE] Support for custom template of notification sends to user to reset password (by vo manager).
- [REGISTRAR] Registration module for eduTEAMS nickname.
- [REGISTRAR] Gather also isCesnetElegibleLastSeen attribute and use it in registration modules for Metacentrum and DU.
- [GUI] Support for foreign proxies (show original identity IdP names) in registrar and profile.
- [API] Allow un/blocking all services on facility/destination.
- [API] Support for SCIM protocol in API.
- [Other] Add error message to listing of TaskResults for destination in CLI.

Changed

- [CORE] Allow Facility deletion, even when blocked service exists.
- [CORE] Move VOMS group names and roles attributes into group-resource like attributes.
- [CORE] Smart sort hostnames in GUI (hosts, destinations, task results).
- [REGISTRAR] Updated BBMRI registration module.

Fixed

- [CORE] Comparison of TaskSchedule improves service provisioning planning.
- [CORE] JSON deserialization of RichMember when synchronizing two perun instances.
- [CORE] Selecting UserExtSource attributes by their names.
- [Other] Compatibility with Java 11.
- [Other] Running test on current Debian (broken OpenJDK).
- [Other] Overall log levels.

2018-10-24

Added

- [CORE] Initial support for group membership expiration.
- [CORE] Support for entities with descriptions containing newlines in audit events and pushing to LDAP.
- [CORE] Possibility to generate graph of attribute dependencies.
- [CORE] Support for alternative login names passed from original IdP, collected in user attribute.

- [CORE] Changed behaviour of attribute modules for elixirBonaFideStatus and eduPersonScopedAffiliations.
- [CORE] Method to get only direct members of Group.
- [CORE] Allow group synchronization of groups in hierarchy (only direct members are synchronized now).
- [REGISTRAR] Added support for group extension forms and workflow.
- [REGISTRAR] Fullback on English texts on registration form if native language is not properly set.
- [GUI] User profile can have native and/or English descriptions for each attribute displayed on profile page.
- [GUI] Link for mail validation during registration can contain "target" param which will be used to redirect user on success.
- [GUI] Allow custom privacy policy link in admin gui footer.
  [API] Method to get Facility or Resource attributes by names.
- [API] Create methods for all base entities. They take specific params instead of entity instance itself.
- [API] GetAllowedRichGroupsWithAttributes() method.
- [API] GetUserExtSourceByExtLoginAndExtSourceName() method.
- [API] GetResourcesWhereUser(Group)IsAdmin() method.
- [API] RemoveAttributes() for member, group and workWithUserAttributes flag.
- [Other] Generic web-app to create own VO.
- [Other] CLI to add/remove members sponsors.
- [Other] CLI to manage attribute R/W rights.
- [Other] Updated Spring to latest version.

Changed

- [CORE] Recalculate attribute dependencies when new attribute is created.
- [REGISTRAR] Extended registration form items content to exceed 4000 chars limitation.
- [Other] To locally run perun we now use cargo maven plugin instead of tomcat7.

Removed

- [Other] All remaining ExecService mentions and usage from code.

Fixed

- [CORE] Failing on empty name when generating login.
- [CORE] Equals on User, Candidate and Member objects.
- [CORE] SQL for batch processing of more than 1000 entities by their IDs.
- [CORE] Getting facility by attribute value.
- [CORE] Passing boolean to jdbc driver on Oracle DB.
- [CORE] Setting From to MimeMessages in notifications.
- [CORE] Escaping input in XML for MU password manager.
- [REGISTRAR] Re-sending of registration notifications from application detail.
- [GUI] Pre-filled mail selection pop-up was covered under other form items.
- [GUI] Do not evaluate HTML in user names.
- [GUI] Loading default tabs for VO managers without VO.
- [GUI] Resolving authorization when opening group in relation on group detail page.
- [GUI] Loading of Groups from proper VO when copying registration form from other VOs/Groups.
- [API] Authorization for fillAttribute() method.
- [Other] Javadoc and RPC API automatic generation, added missing object and examples.

2018-01 - 2018-06

Added

- OAuth2 authentication to Perun API.
- Redundant LDAP endpoint.
- Simplified UI when manually adding users to VOs or Groups.
- Versioning of Perun software.
- Released and deployed Perun 3.1.0.

Changed

- The syntax of groupNames OIDC claim follows AARC recommendation.
- Switched from rolling updates of Perun software to periodic releases.
- Changelog is now maintained per component, providing more detailed information.
- Configurable user-profile page.
- New security measures based on results of penetration testing.
- Provisioning engine performance improvements.

Fixed

- Partial fix for Chrome on Windows using Kerberos authentication.
- Members are no longer validated if membership expiration is set to future and current status is "disabled".
- Notifications about future account expiration are no longer sent, if user has submitted (pending) membership extension application.

2.5.3 Future plans

- Tight integration with Check-in service.
- Support user life-cycle within groups
- New GUI
- Improved UX for the account linking

2.6 WaTTS

2.6.1 Overview

Service/Tool name	WaTTS
Service/Tool url	Prod: https://watts-prod.data.kit.edu Devel: https://watts.data.kit.edu
Service/Tool information page	https://watts-prod.data.kit.edu/docs/user/index.html
Description	WaTTS is a flexible and scalable Token Translation Service, supporting IGTF compatible (IOTA) X.509 certificates.
Value proposition	Allow to (transparently) create X.509 certificates for a user. This makes usage of grid infrastructures easier (user does not see the certificate). This also makes robot certificates superfluous.

Customer of the service/tool	Research Communities
User of the service/tool	End-users accessing R/e-Infrastructure services using either PKIX or a combination of PKIX and SSH credentials.
User Documentation	https://watts-prod.data.kit.edu/docs/user/index.html
Technical Documentation	https://watts-prod.data.kit.edu/docs/code/index.html
Product team	KIT
License	Apache License Version 2.0
Source code	https://github.com/watts-kit/
Testing	Visit page, use plugins: • Info Plugin for minimal testing • X.509 Plugin for X.509 certificate

2.6.2 Release notes

https://github.com/watts-kit/watts/releases

v1.6.2 - 2018-04-04

Fixed

- Fix SSLLABS “F” rating by upgrading to latest version of ERLANG VM
- Remove bad ciphers to get the “A” rating

2.6.3 Future plans

Add fault tolerance, so that operation will not be interrupted, if once instance goes down.

2.7 MasterPortal

2.7.1 Overview

Service/Tool name	MasterPortal (reference service)
Service/Tool url	Multiple instances: https://aai.egi.eu/; https://masterportal-pilot.aai.egi.eu/; https://*elixir*-cilogon-mp.grid.cesnet.cz/; *others*

	SSH proxy access interface: https://aai.egi.eu/sshkeys/
Service/Tool information page	https://wiki.nikhef.nl/grid/AARC_Pilot
Description	Provides a Token Translation capability from (primarily) SAML to X.509 leveraging the RCauth online CA, and enabling pure web-based portals to access X.509 resources on behalf of their users. Transparent caching service between Science Gateways and the RCauth online CA, handling the complexity of obtaining certificates for the Science Gateways and end-users. Additionally provides capability to upload SSH public keys and retrieving proxy certificates using those.
Value proposition	Allowing to use X.509-based credentials, while hiding all the complexity for the end-users. An ancillary capability allows authentication to community portals and science gateways via OpenID Connect for users usually authenticating via SAML (implicit SAML-to-OIDC translation) when used in conjunction with the RCauth.eu operational service.
Customer of the service/tool	Either Science Gateways needing X.509 credentials, or 'power-users' that can leverage SSH key authentication to obtain proxy certificates.
User of the service/tool	End-users accessing R/e-Infrastructure services using either PKIX or a combination of PKIX and SSH credentials.
User Documentation	https://wiki.nikhef.nl/grid/AARC_Pilot_-_SSH_Key_Portal - end-users https://wiki.nikhef.nl/grid/RCAuth.eu_MasterPortal_VOPortal_integration_guide - VOportal developers/operators
Technical Documentation	https://wiki.nikhef.nl/grid/AARC_Pilot
Product team	Nikhef, GRNET
License	Apache License Version 2.0
Source code	https://github.com/rcauth-eu
Testing	Each subcomponent comes with junit tests that are run after each release candidate build. The integration test is performed using a ansibleised virtual container environment (accessibility testing of the operational is performed with nagios from within the operating site)

2.7.2 Release notes

https://github.com/rcauth-eu/aarc-master-portal/releases

2018-09-06

Added

- Add new client auto-registration endpoint (by default disabled)

2.7.3 Future plans

Service capability alignment with WaTTS is ongoing, and although at this point the two token translation services provide slightly different capabilities and a different focus (with the MasterPortal being primarily targeted at community proxy operators that will connect multiple science gateways to a single MasterPortal), it is feasible that both tools evolve in a way that allows merger of the services.

2.8 RCauth - Online CA

2.8.1 Overview

Service/Tool name	RCauth.eu
Service/Tool url	http://pilot-ca1.rcauth.eu/
Service/Tool information page	https://rcauth.eu/
Description	The RCauth.eu service is token translation services (TTS) that can on-the-fly identify entities based on federated credentials and issue to them PKIX credentials in real-time, focussing on converting SAML-to-PKIX. Primarily intended as an operational resource for user and community-facing credential management portals, such as WaTTS and other 'master portals', it provides an OpenID Connect authenticated capability to provide globally trusted PKIX credentials at the DOGWOOD [RFC6711] assurance profile.
Value proposition	Allows token translation services and BPA proxy components to completely hide the use of PKIX credential issuance from the end-user.
Customer of the service/tool	AARC BPA Proxy and token translation service operators on behalf of both Research and generic e-Infrastructures.
User of the service/tool	End-users accessing R/e-Infrastructure services by means of PKIX credentials
User Documentation	MasterPortal operators: https://wiki.nikhef.nl/grid/AARC_Pilot_-_Master_Portal_Administrator_Guide Science GateWay operators/developers: https://wiki.nikhef.nl/grid/RCAuth.eu_MasterPortal_VOPortal_integration_guide End-users: Not applicable
Technical Documentation	https://www.rcauth.eu/tech-resources

Product team	Nikhef, GRNET, STFC
License	Apache License Version 2.0
Source code	https://github.com/rcauth-eu
Testing	Each subcomponent comes with junit tests that are run after each release candidate build. The integration test is performed using a ansibleised virtual container environment (accessibility testing of the operational is performed with nagios from within the operating site)

2.8.2 Release notes

All changes will be logged in the Certificate Practice Statement [R4] of the RCauth.eu service (see Revision History section).

2.8.3 Future plans

The currently-operational RCauth.eu instance is single-homed at Nikhef, where a local cold-standby system is available. To reach the desired service level, it is necessary to distribute the service geographically and move to a full active-active redundant set-up across the federated operators GRNET, STFC, and Nikhef. The software platform (“delegation service”) will be re-engineered to allow for state consistency between a geographically distributed set of instance machines, assuming dedicated, secure, and low-latency virtual private circuits between the hosting sites. The system software for the secure CA has been adapted to support independent distributed operation for up to 256 parallel issuance systems.

3 Marketplace and Order Management tools

3.1 Overview

This chapter provides information on the EOSC-hub business tools in support of the service portfolio management, the order management, the presentation of service level agreements (SLAs, OLAs) to the users and the service reporting.

The Service Portfolio Management Tool (SPMT) provides a full list of services and allows managing service descriptions according to the service management guidelines of FitSM. SPMT manages service descriptions to the granularity of service components and it is designed for following the FitSM service portfolio management process. The SPMT also allows exporting service descriptions to other tools and service catalogues, such as the one to be established by the eInfraCentral project. Production services of EOSC-hub can be displayed by the Marketplace, to be consumed by customers that gather information about available service options and submit an order for a specific service instance or combination of service instances. SLAs are shown basing on the integration with the Operations Portal- Marketplace Backoffice component (see Section 4.2).

3.2 Marketplace

3.2.1 Overview

Service/Tool name	Marketplace
Service/Tool url	https://marketplace.eosc-portal.eu
Service/Tool information page	https://wiki.eosc-hub.eu/display/EOSC/Marketplace
Description	Marketplace (MP) is a user-facing platform where productional EOSC-hub services can be promoted, discovered, ordered and accessed. A set of functionalities implemented in Marketplace supports efficient order management and facilitates the interactions of user with e-infrastructures.
Value proposition	Common platform to facilitate activities of service users, customers and providers in scope of EOSC services. It provides functionality to support full user path between service discovery and service access. It brings an environment for service providers to appropriately manage offers of their resources and services. It follows best practices of UX to ensure best user experience.
Customer of the service/tool	Researchers, Research Groups, Business Representative
User of the service/tool	Researchers, Research Groups, Business Representatives, Service Owners, Service Providers

User Documentation	https://wiki.eosc-hub.eu/display/EOSC/User+manual (Work In Progress)
Technical Documentation	https://github.com/cyfronet-fid/marketplace
Product team	ACC Cyfronet AGH
License	Apache License Version 2.0
Source code	https://github.com/cyfronet-fid/marketplace
Testing	Unit and Integration testing integrated within the MP RoR application is a part of development and deployment process (Travis CI based). The code review is a part of the development process. Functional and user interface testing is being held before every release. New features are approved by WP2 & WP4 before being released in Production.

3.2.2 Release notes

https://github.com/cyfronet-fid/marketplace/blob/master/CHANGELOG.md

1.0.0 - 2018-12-20

Added

- New visual identity (EOSC Portal)
- Service Ranking functionality
- JIRA integration
- Filtering functionality based on static attributes
- Project Item artefact - custom view to manage service order after issuing (communication with the service provider)
- “Ask a Question about the Service” functionality

Changed

- 3-step ordering process
- new implementation of service offers (service options)
- new categorisation model: 1-level categorisation tree + filters within the service category

3.2.3 Future plans

- Integration with SPMT
- Integration with GOCDB
- Integration with DPMT
- Enhancements in JIRA integration
- Enhancements in the ordering process
- GUI enhancements basing on users’ feedback

3.3 Service Portfolio Management Tool (AGORA)

3.3.1 Overview

Service/Tool name	AGORA/SPMT
Service/Tool url	https://eosc.agora.grnet.gr & https://eosc-hub-devel.agora.grnet.gr
Service/Tool information page	https://grnet.github.io/agora-sp/
Description	The Service Portfolio Management Tool (SPMT/AGORA) provides a full list of services and allows managing service descriptions according to the service management guidelines of FitSM.
Value proposition	It manages service descriptions to the granularity of service components and according to the service management guidelines of FitSM. The SPMT also allows to export service descriptions to other tools and service catalogues, such as the one to be established by the eInfraCentral project and https://www.eosc-hub.eu/catalogue
Customer of the service/tool	Service Providers, Resource Provider; Research Communities
User of the service/tool	Service Providers, Service Portfolio Managers
User Documentation	https://grnet.github.io/agora-sp/
Technical Documentation	https://grnet.github.io/agora-sp/
Product team	GRNET
License	AGPL-3.0
Source code	https://github.com/grnet/agora-sp https://github.com/grnet/agora-sp-admin https://github.com/grnet/agora-probes https://github.com/grnet/agora-catalogue-react-view
Testing	Unit and Integration testing is performed on the Staging instance (https://eosc-hub-devel.agora.grnet.gr) New features are approved by WP2 & WP4 before being released in Production.

3.3.2 Release notes

Agora Backend

Unreleased

Added

- Add service-types endpoint.
- Push messages using Argo Messaging Service

Changed

- Expose funders_for_service to api/v1
- Enable filtering of service versions by is_in_catalogue

Security

- Upgrade Django to 1.11.16.

0.9.6 - 2018-09-25

Added

- Clean html feature for rich text textarea fields.

0.9.5 - 2018-08-28

Changed

- Add field "service_type" in CIDL model.

Fixed

- Add forgotten migration file.

0.9.4 - 2018-07-06

Changed

- Upgrade APIMAS
- Update spec and permissions file according to new APIMAS

Added

- Add serviceowner role
- Add service ownership functionality
- Allow service filtering for user customers
- Expose service customer_facing/internal attributes
- Expose external services in api

Fixed

- Remove duplicate code from spec.
- Enable custom user creation from UI

0.9.3 - 2018-04-11

Added

- Add superadmin role.
- Enable service logo upload.
- Dockerize app.
- Add tests.

Changed

- Properly set up permissions for admin/observers.

Fixed

- Remove unused settings.

0.9.2 - 2018-01-31

Fixed

- Clean up unsafe code

Added

- Enable user login via shibboleth.
- Send email when a new user is created.
- Expose shibboleth_id in api.
- Expose component-implementation-detail-link endpoint.
- Expose service component in api.

Changed

- Expose user shibboleth_id in api.
- Allow filtering of resources.

3.3.2.1 Agora Admin-UI

Unreleased

Deprecated

- Migrate away from bower

Changed

- Enable filtering of service versions by is_in_catalogue

0.9.4 - 2018-08-28

Added

- "View source" mode in textarea fields.

Changed

- Add field "service_type" in CIDL model
- Update menu labels in "Service Components" section

Fixed

- Remove duplicate code from CIDL.
- Eslint fixes.
- Bug concerning user creation.

0.9.3 - 2018-07-06

Added

- Allow custom-user create/edit.
- Add role serviceowner.
- Implement service ownership functionality.

Changed

- Use PATCH to upload image to backend

Fixed

- Fix typos

0.9.2 - 2018-04-11

Added

- Allow service-item logo upload.
- Add role field to custom-user.
- Add superadmin/admin roles.
- Add customer_facing/external attributes to services.

Changed

- Replace froala text editor with tinyMCE

0.9.1 - 2018-01-26

Added

- Initial version for EOSC-HUB
- Implement file upload
- Enable shibboleth login

3.3.2.2 Agora Drupal-Connector

1.3 - 2018-10-25

Changed

- Update React plugin to latest changes

1.2 - 2018-07-20

Added

- Support for Multiple Feeds

3.3.2.3 ***agora-catalogue-react-view***

1.0.0 - 2018-09-27

Security

- Updated lodash version to 4.17.11

0.9.0 - 2018-07-20

Added

- Support for Multiple Feeds

3.3.3 Future plans

- Provide an api for the CMDBs (GOCDB and DMPT) to get list of approved the service_types
- Integrate with Marketplace,
- Add In_Marketplace flag to Service Versions.
- Adapt service model according to the instructions of WP2

4 Integrated Business and Operations Support Systems

4.1 Overview

This chapter provides the overview, release notes and future plans for the Operations Portal, the Data Project Management Tool (DPMT), the Data Management Planning Tool (DMPT), the information repository (GOCDB) and the Service Versions Monitoring (SVMON).

The services discussed in this chapter facilitate the EOSC-hub operations, configuration and change management as well as distributed order management processes. The main objective during the initial period of the project was the establishment of work plans for integration of these services with other services within work package 5 like Service Portfolio Management Tool, Marketplace, and Accounting Repository etc. Many integration plans have been successfully implemented and the integration goals have been achieved. The detailed results and achievements will be given in the next deliverable D5.3.

4.2 Operations Portal

4.2.1 Overview

Service/Tool name	Operations Portal
Service/Tool url	http://operations-portal.egi.eu http://operations-portal.egi.eu/vapor
Service/Tool information page	https://wiki.egi.eu/wiki/Operations_Portal
Description	The Operations Portal provides VO management functions and other capabilities which support the daily operations of EGI. It is a central portal for the operations community that offers a bundle of different capabilities, such as the broadcast tool, VO management facilities, different dashboards that are used to display information about failing monitoring probes and to open tickets to the Resource Centres affected. The dashboards also support the central grid oversight activities. It is fully interfaced with the EGI Helpdesk and the monitoring system through messaging. The Operations Portal provides tools supporting the daily running of operations of the entire infrastructure: Infrastructure oversight, security operations, VO management, broadcast, availability reporting.
Value proposition	• Improve and enrich existing tools • Adapt or develop tools with needs expressed by new communities • Adapt or develop tools within the evolution of the EOSC environment

Customer of the service/tool	RI; Resource Provider; Research Communities; Virtual Organisations
User of the service/tool	Site admins; Operations Managers; Virtual Organisations; large research group
User Documentation	https://forge.in2p3.fr/projects/opsportalmaster?jump=wiki
Technical Documentation	https://forge.in2p3.fr/projects/opsportalmaster?jump=wiki
Product team	CNRS
License	Apache License Version 2.0
Source code	https://gitlab.in2p3.fr/opsportal/sf3
Testing	Automated Tests : https://forge.in2p3.fr/projects/opsportaluser/wiki/Continuous_Integration Release procedure : https://wiki.egi.eu/wiki/PROC23

4.2.2 Release notes

VAPOR_2.5 - 2018-11-20

Fixed

- issue 6205 Problem with icons in the tree
- issue 6204 Resources Explorer for the Top Bdii is not working properly
- issue 6203 Sites details in Figures page - the breadcrumb is broken
- issue 6186 "View errors" button is not visible into JobMonitoring
- issue 6185 Headers of cards are broken into JobMonitoring
- issue 6184 Differences into the form Job Monitoring
- issue 5575 Fix the problem with the shifted table layout

Changed

- issue 6651 Upgrade Lavoisier Server
- issue 6187 Improve DataManagement pages
- issue 5574 Upgrade Bootstrap Cyril L'Orphelin closed
- issue 5573 Add the selection of the numbers of entries in the Job Monitoring

4.2.3 Future plans

- Achieve the Operations Dashboard to replace the different existing dashboards [R5]
- Achieve the AAI integration
  - integrate new authorization rules - especially for users from EUDAT B2ACCESS, VO Membership
  - Use the unique identifier as reference
- Service Order Management Tool [R6]

4.3 GOCDB

4.3.1 Overview

Service/Tool name	GOCDB
Service/Tool url	https://goc.egi.eu
Service/Tool information page	https://wiki.egi.eu/wiki/GOCDB
Description	GOCDB is a central registry to record information about the topology of an e-Infrastructure. This includes entities such as resource centers (sites), services, service-endpoints and their downtimes, contact information and roles of users responsible for operations at different levels. The service enforces a number of business rules and defines different grouping mechanisms including object-tagging for the purposes of fine-grained resource filtering.
Value proposition	GOCDB is a key tool for the configuration management of the EGI Federation and WLCG. It is a definitive information source, with the emphasis on user communities to maintain their own data. It is intentionally designed to have no dependencies on other operational tools for information.
Customer of the service/tool	EGI Operations and WLCG
User of the service/tool	Site/service admins, NGI managers and Security teams
User Documentation	https://wiki.egi.eu/wiki/GOCDB
Technical Documentation	https://wiki.egi.eu/wiki/GOCDB
Product team	UKRI-STFC
License	Apache License Version 2.0
Source code	https://github.com/GOCDB/gocdb
Testing	Before every production release, GOCDB development is frozen and a period of testing is announced that lasts for approximately two weeks to one month using the GOCDB test instance. This testing phase is widely disseminated using the relevant mail lists, and all operational tools and

	users are invited to perform tests against this instance.

4.3.2 Release notes

5.7.2.2 - 2018-05-11

Fixed

- Validation of service host DNs

5.7.2.0 - 2018-04-03

Added

- Notify flag on sites and services

5.7.1.0 - 2018-02-02

Changed

- Documentation updates

Security

- Patch for minor issue

4.3.3 Future plans

- Development of an EOSC-hub specific view on the data in GOCDB.
- Change in the underlying infrastructure of GOCDB to improve reliability.
- Update to site map on main page.

4.4 Data Project Management Tool

4.4.1 Overview

Service/Tool name	Data Project Management Tool (DPMT)
Service/Tool url	https://dp.eudat.eu
Service/Tool information page	https://github.com/EUDAT-DPMT
Description	DPMT is EUDAT’s internal coordination tool. Information about providers and customers as well as the projects that they are engaged in are documented in DPMT. EUDAT’s currently running services, service components and resources provided through them are registered with the DPMT.

Value proposition	DPMT is a web-based portal application designed to allow new and existing data projects to be enabled, managed and monitored with the help of the partners of the EUDAT CDI. Machine agents can gather information about all EUDAT services, service components and resources through an API that is compatible with the GOCDB API (see above). A central deployment of the DPMT serves the entire EUDAT CDI reducing the maintenance costs. Through multiple, taylormade interfaces it supports easy and effective interoperability with EOSC's operational tools.
Customer of the service/tool	EUDAT's Service and Resource Providers; Research Communities
User of the service/tool	Site admins; Operations Managers; Project PIs; Community Managers
User Documentation	https://dp.eudat.eu/help/
Technical Documentation	https://github.com/EUDAT-DPMT and https://gitlab.mpcdf.mpg.de/rjr/dpmt-config/wikis/operation (not public)
Product team	MPCDF
License	GPL Version 2.0
Source code	https://github.com/EUDAT-DPMT
Testing	MPCDF operates a development instance of the DPMT where all new features and components can be demonstrated and tested before they are rolled out in production.

4.4.2 Release notes

The DPMT is based on the Plone [R7] content management system. The custom content types used to describe the main DPMT concepts are defined in a Plone add-on called pcp.contenttypes which is available from GitHub [R8].

2018-06-27

Changed

- Suppress right column on accounting view for RSR.

2018-06-20

Changed

- Turning stuff like '6.92e+14' into '692000000000000'

2018-06-19

Changed

- Adding site information to star record.

- Convert all storage usage values to byte

2018-05-29

Changed

- Add review state to extensions and be a bit more defensive against missing vocab entries

2018-05-16

Changed

- Match ARGO's expectation of what's where

2018-04-26

Changed

- Adding classification and severity to GOCB view of downtimes
- Further compatibility tweaks

2018-04-25

Changed

- Further improvements towards GOCDB compatibility
- Introducing a typo (sic) to become compatible with GOCDB

Fixed

- Fixing typo in classification

2018-04-13

Fixed

- Correct typo

Changed

- Extend provider overview to include more info
- Extending downtime schema. Expects vocabularies 'severity_levels' and 'downtime_classes' to be around.

Added

- Adding provider to downtime overview

2018-04-11

Changed

- List star records for all RSR on site root

Fixed

- Substructure template and don't break on missing records

2018-04-06

Fixed

- Don't break if no contact is specified

Changed

- When displaying a term from a vocabulary - here for service types - use the title rather than the id.

Added

- First pass at adding further content. May need to become a bit more defensive.
- There is now a minimal star record for registered storage resources
- Basic skeleton of 'star' view for registered storage resources
- Basic skeleton for 'service group view' a la GOCDB

4.4.3 Future plans

Deeper integration of DPMT into the forthcoming EOSC operational infrastructure requires more functionality of the DPMT to be accessible by machine agents; most notably write operations. To this end it is planned to incorporate (and adjust where necessary) an add-on to the underlying web framework Plone that exposes the full functionality through a hypermedia style REST API [R9].

4.5 Data Management Planning Tool

4.5.1 Overview

Service/Tool name	EasyDMP
Service/Tool url	https://easydmp.eudat.eu
Service/Tool information page	https://www.sigma2.no/content/easydmp
Description	EasyDMP is an EUDAT tool for creating data management plans. The tool also makes use of the EESTORE that is a service providing a uniform interface to information from third-party registries that are required when completing a data management plan.
Value proposition	Provides a configurable web interface that makes it easier for researchers to create data management plans. The intention is to further integrate with EUDAT services to allow provision of services as part of the creation of the data management plan rather than having the two activities (creating a plan and provisioning services) separated. This will also enable the plan to be verified at a later date (ie is the project following the approved plan).
Customer of the service/tool	Researchers, Resource providers
User of the service/tool	Researchers
User Documentation	https://www.sigma2.no/easydmp/how-to
Technical Documentation	https://github.com/hmpf/easydmp https://gitlab.eudat.eu/dmp/eestore
Product team	Sigma2 (EOSC-Hub), Athena Research and Innovation Centre (OpenAIRE)

License	MIT
Source code	https://github.com/hmpf/easydmp https://gitlab.eudat.eu/dmp/eestore
Testing	The code makes use of the Django unit test framework. The tests are run before each release. New tests are created based on feedback from users.

4.5.2 Release notes

Release information is maintained in [R10].

0.12.3 - 2018-11-15

Fixed

- Bugfixes: relating to the viewer role after 0.12.1
- Bugfixes: relating to what pages should be public after 0.12.1

Added

- Added a themed Not Found page.

0.12.2 - 2018-11-05

Changed

- Add links to EUDAT's TOS and Privacy Policy in the footer.

0.12.1 - 2018-10-26

Fixed

- Bugfix: Users were not redirected to the login page when accessing a plan anonymously but got a 500 server error instead.
- Bugfix: Not all the necessary authentication backends were in use.
- Other small fixes

0.12 - 2018-10-18

Added

- Backend-support for logging of events
- Usage of JWT for access to non-public parts of the API.

Changed

- Switch from homebrew auth system for templates to django-guardian.

0.11.1 - 2018-09-26

Added

- Support for docker-compose to ease development. This includes fixtures to fill the database with the relevant user types (superuser, ordinary user) and a sample template. This isn't end-user relevant or run-time bug prone so is relegated to a patch-version.

0.11 - 2018-09-21

Added

- A very rudimentary system for giving people usage access to unpublished templates, for ease of cooperative development of new templates.

0.10 - 2018-09-14

Changed

- Overhaul of the invitation system

Added

- New user role for plans: view only

2018-09

Changed

- Easy and not so easy speed optimizations.
- Changes to allow for easier on-boarding of new developers.

2018, first half

Changed

- New look and many UI-improvements for end users.
- Most templates made private.

4.5.3 Future plans

The work on the tool for data management plans is being done in collaboration with OpenAIRE. EasyDMP is the tool created under the EUDAT project. The openAIRE-EOSC-HUB tool is called openDMP. Both tools are under active development. 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.

4.6 Service Versions Monitoring Tool

4.6.1 Overview

Service/Tool name	SVMON
Service/Tool url	https://svmon.eudat.eu
Service/Tool information page	https://wiki.eosc-hub.eu/display/EOSC/SVMON+Description (in progress)
Description	SVMON collects software versions of EUDAT services and their corresponding components in EUDAT CDI.
Value proposition	SVMON collects information on software versions, stores and displays collections in a compact view. SVMON also uniquely provides information of service attributes.
Customer of the service/tool	EOSC-hub customers
User of the service/tool	EUDAT service providers, site administrators

User Documentation	https://gitlab.eudat.eu/jie.yuan/svmon-app/blob/master/manual (in progress)
Technical Documentation	https://gitlab.eudat.eu/jie.yuan/svmon-app/blob/master/README.md (in progress)
Product team	KIT
License	Apache License 2.0 The MIT License Copyright (c) 2014-2018 Google, Inc.
Source code	https://gitlab.eudat.eu/jie.yuan/svmon-app
Testing	Unit test, functions test on testing instance (https://svmon-dev.scc.kit.edu)

4.6.2 Release notes

1.0.3 - 2018-09-18

Added

- implement more service components in svmon client, more API endpoints

Fixed

- pakiti report parser

Removed

- Spring thymeleaf dependency

1.0.2 - 2018-07-18

Added

- implement authentication layer with username and B2ACCESS OAuth2.0

Fixed

- Angular page refreshing

Changed

- Angular front with true authentication and authorization

1.0.1 - 2018-04-18

Added

- support Pakiti client, SVMON client, deploy httpd proxy with https protocol

Changed

- integrate with GOCDB and DPMT

1.0.0 - 2018-03-18

Changed

- first release

4.6.3 Future plans

- Include more sites and hosts
- Distribute SVMON client on hosts

5 Monitoring, Accounting, Messaging and Security Tools

5.1 Overview

This Chapter provides the overview, release notes and brief future plans for the ARGO Availability and Reliability Monitoring Service, Argo Messaging, Accounting Repository, Accounting Portal and Security Tools. Many integration plans have been successfully implemented and the integration goals have been achieved. The detailed results and achievements will be given in the next deliverable D5.3.

5.2 Accounting Repository

5.2.1 Overview

Service/Tool name	APEL
Service/Tool url	http://apel.github.io/
Service/Tool information page	https://wiki.egi.eu/wiki/Accounting_Repository
Description	The Accounting Repository 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 available through the Accounting Portal.
Value proposition	Combined reporting of EGI and EUDAT storage resource usage, giving unified EOSC-hub usage accounting. Improvements to the client-side software making it easier to operate and enabling problems to be diagnosed more rapidly.
Customer of the service/tool	RI; Resource Provider; Research Communities
User of the service/tool	Site admins; Operations Managers; large research groups
User Documentation	https://wiki.egi.eu/wiki/APEL
Technical Documentation	https://wiki.egi.eu/wiki/APEL
Product team	STFC

License	Apache License, Version 2.0
Source code	https://github.com/apel/apel (client and server software) https://github.com/apel/ssm (messaging tool)
Testing	The APEL project uses a development workflow based around GitHub, which includes a semi-automatic testing procedure used to assess the quality of software releases. This procedure comprises automated unit tests and code quality checks, peer review, test builds, testing on a pre-production system, and deployment to test sites.

5.2.2 Release notes

apel-1.7.0 - 2018-06-05

Added

- Long running VM support to the server: Cloud VMs that run over month boundaries will now have their usage in each month assigned to the correct month.

apel-1.6.2 - 2018-04-16

Changed

- Added all job statuses to the SLURM log parser that indicates the job has stopped and that resources have been used so that more types of completed job are accounted for.

Fixed

- CpuCount being NULL in cloud accounting records and leading to warnings when summarising.

Removed

- References to specific LSF versions in the documentation as all versions are now allowed.

apel-ssm-2.3.0 - 2018-08-16

Added

- Support for stomp.py versions from 3.1.6 onwards which allows for builds on Ubuntu Trusty and should enable IPv6 support.
- Script for creating Ubuntu (.deb) builds.
- Script for creating Docker container builds.

apel-ssm-2.2.1 - 2018-05-14

Added

- Check that the server certificate used for encryption hasn't expired so that a sending SSM won't start with an out of date server certificate.

Changed

- Error handling for received messages so that more useful debugging information in obtained.

5.2.3 Future plans

- Roll out support for the Argo Messaging Service (AMS).
- Enhancements to storage accounting.
- Ensure SAML authentication is supported in the accounting records.

- New interface and API for publishing and synchronisation tests.

5.3 Accounting Portal

5.3.1 Overview

Service/Tool name	EGI Accounting Portal
Service/Tool url	https://accounting.egi.eu/
Service/Tool information page	https://wiki.egi.eu/wiki/Accounting_Portal
Description	The Accounting Portal provides data accounting views for users, VO Managers, NGI operations and the general public.
Value proposition	The Accounting Portal acts as an interface to different accounting records, integrating them with other data and metadata from several providers and presents a homogeneous view of the data gathered and a user-friendly access.
Customer of the service/tool	VO Managers, NGI operations and the general public
User of the service/tool	VO Managers, NGI operations and the general public
User Documentation	https://accounting.egi.eu/static/EGI%20Accounting%20Portal%20User's%20Guide.pdf
Technical Documentation	https://wiki.egi.eu/wiki/Accounting_Portal_API
Product team	CESGA
License	Apache License Version 2.0
Source code	https://github.com/cesga-egi/accounting
Testing	Testing using development version and pre-production version by a dedicated EGI Operations Tools Advisory Group

5.3.2 Release notes

- EUDAT integrated portal instantiate with streamlined information (no VOs), and EUDAT specific verbal requirements.
- Renaming WLCG metrics.

- Improved unit handling.
- Fix bug for month periods in GMT- hemisphere.
- Improved Tier 1 PDF reports.
- Continuity plan testing.
- Added EUDAT “fake” topology.
- Change date handling on storage accounting.
- Solved CSV Content-Disposition filename problems with Firefox.
- Changed Topology JDBC endpoint.
- Improved gocdb3_1h presentation and removed unwanted warnings.
- Fixes to JSON/CSV API.

5.3.3 Future plans

- Finalise AAI integration, which is currently under testing.
- Provide new dedicated instance for implementing EUDAT requirements that require a heavy streamlining of the service that would hide relevant information for many actors.

5.4 Monitoring

5.4.1 Overview

Service/Tool name	ARGO Monitoring
Service/Tool url	http://argo.egi.eu
Service/Tool information page	https://wiki.egi.eu/wiki/ARGO
Description	ARGO is a flexible and scalable framework for monitoring status, availability and reliability
Value proposition	ARGO provides monitoring of services, visualization of the their status, dashboard interfacing, notification system and generation of availability and reliability reports. The dashboard design enables easy access and visualisation of data for end-users. Third parties can gather monitoring data from the system through a complete API. A central deployment of the ARGO monitoring engine can serve a large infrastructure reducing the maintenance costs.
Customer of the service/tool	RI; Resource Provider; Research Communities
User of the service/tool	Site admins; Operations Managers; large research group
User Documentation	http://argoeu.github.io; http://argo.egi.eu

Technical Documentation	http://argoeu.github.io
Product team	GRNET, SRCE, CNRS
License	Apache License Version 2.0
Source code	https://github.com/ARGOeu/
Testing	ARGO Monitoring follows a development process where tests that check the functionality and the quality, correctness of the software are mandatory. This process consists of automated unit tests and code quality checks, running via a CI tool (jenkins). All main components (where applicable) of ARGO monitoring follow the same approach. The types of tests are: • [Connectors] - Unit tests for all different functionalities for connectors. • [POEM] - There are currently two apps in Poem project: poem and api. For both of these apps unit tests (python) that test the functionality are supported. • [Compute Engine] - End-to-end *testing* of all *Flink jobs.* Unit tests for batch and streaming jobs of the compute engine. • [WEB-API] - 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) • [WEB-API] - External test: Web API endpoints are tested as postman collections via newman. Newman [R11] is a command-line collection runner for Postman [R12]. It allows you to effortlessly run and test a Postman Collections [R13] 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. • [argo-alerts] - Unit tests that gather data from GOCDB and create contact lists to send the alerts.

5.4.2 Release notes

5.4.2.1 ams-consumer

V1.1.0.0-1 - 2018-05-10

- ARGO-1106 Pull interval as float
- ARGO-1092 AMS Consumer README
- ARGO-1069 AMS Consumer Centos7 support
- ARGO-1050 Connection timeout as config option
- ARGO-869 RPM packaging metadata
- ARGO-1036 report period fix
- ARGO-1036 Message retention logic
- ARGO-790 avro serialization of fetched data

- ARGO-971 AMS messages fetching loop
- ARGO-846 Introduce config parser with template config file
- ARGO-845 Daemonize worker process and register signal handlers

V0.1.0-1 - 2018-02-20

- RPM package

5.4.2.2 *argo-alert*

V0.1-2 - 2018-11-09

- ARGO-1464 Update requests dep to 2.20

V0.1-1 - 2018-02-27

- ARGO-1402 Enable status-streaming job per report
- ARGO-919 Alerta publish to AMS plugin
- ARGO-1175 Refactor rulegen to ingore empty notification elements
- ARGO-1068 Add argo ui link into alerts
- ARGO-1116 Fix handling of optional params: group-type, timeout
- ARGO-1091 Fix argo-alert-publisher handling of timeout & grouptype args
- ARGO-1075 Refactor notification messages and settings
- ARGO-1066 Add basic http auth support in rule generator
- ARGO-996 Add ability to generate rules using a group of test email destinations
- ARGO-1026 Support different levels of entity groups when retrieving contact information
- ARGO-1002 Set Content-Type header when publishing to alerta
- ARGO-999 Add boolean conf parameter for using contact notifications flags or not
- ARGO-994 Use defusedxml in parsing
- ARGO-990 Accept a list of kafka endpoints for publisher

5.4.2.3 *argo-ams-library*

V0.4.1-1 - 2018-06-19

- ARGO-1120 Extend AMS client to support X509 method via the authentication server

V0.4.0-1 - 2018-05-14

- ARGO-1103 Handle non-JSON AMS responses
- ARGO-1105 Extend ams library to support offset manipulation
- ARGO-1118 Fix returnImmediately parameter in sub pull request
- ARGO-1127 Wrap offsets low level methods into one
- ARGO-1153 Extract JSON error messages propagated through AMS

5.4.2.4 *Argo-egi-connectors*

V1.7.0-1 - 2018-05-23

- ARGO-1093 Support for GOCDB paginated topology API
- ARGO-1080 add support for basic-auth in Connectors
- ARGO-966 Lower state files permissions

V1.6.1-1 - 2018-03-27

- selectively use GOCDB paginated API for topology

5.4.2.5 *Argo-nagios-ams-publisher*

V0.3.1-1 - 2018-06-19

- ARGO-1250 Inspection local socket is left with root permissions
- ARGO-1147 AMS publisher to add optional field
- ARGO-986 Purger should not try to remove non-existing cache msg

V0.3.0-1 - 2018-03-27

- ARGO-1084 Connection settings per topic publisher

- ARGO-1023 Send messages to prod and devel AMS instance in parallel
- ARGO-1055 Last time stats report not updated
- ARGO-1051 Ensure service stop called on system shutdown
- ARGO-1004 UTC timestamp instead of localtime for dispatched results
- ARGO-978 Add systemd init script
- ARGO-806 AMS Publisher nagios testing method for upcoming probe

5.4.2.6 Argo-ncg

V0.4.4 - 2018-06-19

- AO-363 Add eu.egi.sec.dCache-3.0 metric

- AO-331 Deploy ams-publisher Nagios sensor
- AO-360 Propagate attributes from GOCDB extensions
- AO-356 Add dependency to argo-ncg
- ARGO-1247 ncg.reload.sh should clear hanging ncg.pl
- AO-356 Add dependency to argo-ncg
- ARGO-973 Monitoring for OCCI incorrectly rebuilds URL of service with port
- ARGO-1146 Nagios to send actual data
- AO-323 ncg.reload.sh using wrong nagios path
- ARGO-1109 Enable dpmt to monitoring engine
- ARGO-1081 add support for basic-auth

V0.4.3 - 2018-03-27

- ARGO-1070 Implement certificate monitoring for EGI ops tools
- ARGO-1094 Reconfigure nagios to deliver metric results to prod and devel caches
- ARGO-1070 Implement certificate monitoring for EGI ops tools
- AO-323 ncg.reload.sh using wrong nagios path
- AO-322 New version of Nagios raises warning for retry_check_interval
- AO-320 NCG cannot connect to SSL endpoints
- AO-309 Add new WMS probe
- AO-307 Monitor size of AMS publisher local cache.
- ARGO-927 Test AAI CheckIn integration with OpenStack probe

5.4.2.7 Argo-streaming

V1.1 - 2018-10-30

- ARGO-1464 Update requests dep to 2.20
- ARGO-1063 AMS Client logging on issues
- ARGO-1441 Fix hdfs_user param in config scripts
- ARGO-1434 Make check tenant status look back in time for sync data Fix absolute paths in update cron script Upload default empty recomputation profile if missing from HDFS
- ARGO-1403 Create argo-engine update wrapper
- ARGO-1430 Fix sync bugs in automation scripts
- ARGO-1404 Ignore metric data from services that are not included in aggregation profile
- ARGO-1402 Enable streaming-status job per report
- ARGO-1291 Recomputation handling in streaming engine
- ARGO-1298 Upload tenant configuration status to argo-web-api
- ARGO-1290 Create tenant status check script
- ARGO-1392 Argo engine cli script fixes
- ARGO-1065 Establish a fixed restart strategy for streaming jobs
- ARGO-1292 Update AMS project from argo-web-api tenant info
- ARGO-1289 Update crontab for all tenants and their reports

- ARGO-1288 Update tenant reports from argo-web-api
- ARGO-1287 Update tenant list from argo-web-api
- ARGO-1308 Refactor submit scripts to use new configuration
- ARGO-1319 Fix missing status generation issue in batch status job
- ARGO-1286 Parse and separate manual and automatic sections of argo-streaming conf
- ARGO-1277 Check and update thresholds profiles from argo-web-api
- ARGO-1276 Update batch submit scripts to handle threshold params
- ARGO-1274 Refactor ConfigManager to parse topology_schema and filter_tag fields
- ARGO-1273 Refactor aggregation profile parser
- ARGO-1256 Implement Threshold component in batch jobs
- ARGO-1261 Implement Threshold Manager
- ARGO-1149 Refactor batch jobs to accept new metric data schema
- ARGO-1241 Refactor Ingest Metric job to accept extra data

V1.0 - 2018-06-13

- ARGO-1243 Fix recomputation list initialization in batch_ar
- ARGO-1239 Refactor Operations Profile Manager to read new schema
- ARGO-1233 Fetch latest report cfg from argo-web-api
- ARGO-1231 Fetch latest aggregations profile from argo-web-api
- ARGO-1230 Fetch latest ops profile from argo-web-api
- ARGO-1221 Report name capitalization fix
- ARGO-1164 Add downtime feed to streaming status
- ARGO-1163 Fix close on Specific Avro Writer
- ARGO-1156 Refactor flink submissions scripts with updated execution parameters(proxy and ssl)
- ARGO-1160 Fix StatusManager Aggregation Initialization Bug
- ARGO-1083 Streaming status job timeout and multiple-group fixes
- ARGO-1107 Refactor AMS source / connector to support proxy option
- ARGO-1042 Create Status Streaming sumbit script
- ARGO-1041 Create Status job submit script
- ARGO-1074 Add reference to config template relative to each test file
- ARGO-1073 Add more verbose names to flink jobs
- ARGO-1072 Batch status read report cfg
- ARGO-1040 Create A/R job submission script
- ARGO-1067 Fix job sumbit when 0 job run in cluster
- ARGO-1039 Create Sync Ingestion submission Script
- ARGO-1038 Create Metric Ingestion Submit Script
- ARGO-1038 Create Metric Ingestion Submit Script
- ARGO-1044 Fix Downtime handling in compute ar batch job
- ARGO-1000 Remove hardcoded default parallelism from streaming status job env
- ARGO-992 Fix hdfs instance handling in ingest sync job
- ARGO-988 BucketSink: Inacticity threshold increase to 30 minutes
- ARGO-969 Add ability to configure AMS source ingestion rate in flink jobs
- ARGO-983 Implement and use direct Mongo Output Format for storing status batch results
- ARGO-982 Implement and use direct MongoOutputFormat for ar batch results
- ARGO-979 Refactor Metric Ingestion fix datetime buckets at HDFS

*5.4.2.8 **Argo-web-api***

V1.7.8-2 - 2018-11-07

- ARGO-1435 Fix configuration_profile json field in tenant status call
- ARGO-1433 Add tenant status roles to init db script
- ARGO-1268 Serve topology statistics per report
- ARGO-451 Close status timelines with latest daily result

V1.7.7-1 - 2018-09-18

- ARGO-1390 API CALL - Update recomputation
- ARGO-1389 API CALL - Delete Recomputation
- ARGO-1395 Operations profile name field should be unique
- ARGO-1396 Metric profile name field should be unique
- ARGO-1394 Aggregation profile name field should be unique

V1.7.6-1 - 2018-09-12

- ARGO-1298 Show/Update tenant's argo-engine status

V1.7.5-1 2018-09-12

- ARGO-1381 Api call update report name field not unique
- ARGO-1388 Api call update tenant name field
- ARGO-1345 update Tenant model to handle field roles
- ARGO-1391 Wrong response for empty factors list
- ARGO-1381 Refactor error messages in argo-web-api thresholds package

V1.7.4-1 - 2018-09-04

- ARGO-545 Add api call for latest non-ok entries

V1.7.3-1 - 2018-09-04

- ARGO-1380 Refactor error messages in argo-web-api tenants package
- ARGO-1337 Refactor error messages in argo-web-api factors package
- ARGO-445 Recomputation details error
- ARGO-1379 Refactor error messages in the reports package

V1.7.2-1 - 2018-08-21

- ARGO-1351 Refactor error messages in the aggregation profiles package
- ARGO-1349 Refactor error messages in the metric profiles package
- ARGO-1346 Refactor error messages in the opperations package
- ARGO-1275 Refactor Report resource schema
- ARGO-1260 Implement CRUD on threshold profiles resource
- ARGO-1099 Add read-only super-admin

5.4.2.9 poem

V1.2.0-3 - 2018-05-15

- Merge pull request #88 from ARGOeu/devel
- centered delete view
- show only username on history view
- configurable SAML button login string

V1.2.0-1 - 2018-05-10

- HttpAuth disabled by default
- use HttpAuth in service type sync if enabled
- added HttpAuth config options
- Revision templates with proper breadcumb
- removed empty files from source tarball building

V1.1.0-1 - 2018-02-06

- num of tuples only on change view
- place to separated line

5.4.3 Future plans

Support, maintain, extend the Argo Monitoring service according to the workplan defined, including:

- One Stop Shop
- Customer Defined Thresholds
- Unified View

5.5 Argo Messaging Service

5.5.1 Overview

Service/Tool name	ARGO Messaging Service (AMS)
Service/Tool url	http://argoeu.github.io
Service/Tool information page	https://wiki.egi.eu/wiki/Message_brokers
Description	AMS enables reliable asynchronous messaging for the EOSC-hub infrastructure
Value proposition	AMS provides a scalable HTTP Messaging Service with: • An HTTP API for client access • Transparent scalability & high availability • Access controls implemented at the API layer • Multi-tenant support • Instrumentation at the API layer
Customer of the service/tool	NGI; RI; Resource Provider; Research Communities
User of the service/tool	Site admins; Operations Managers; large research group
User Documentation	http://argoeu.github.io;
Technical Documentation	http://argoeu.github.io
Product team	GRNET, SRCE
License	Apache License Version 2.0
Source code	https://github.com/ARGOeu/
Testing	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). The types of tests are: • 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) • External test: AMS endpoints are tested as postman collections via newman. Newman [R11] is a command-line collection runner for Postman [R12]. It allows you to effortlessly run and test a Postman Collections [R13] 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 Release notes

5.5.2.1 argo-messaging

The Messaging Service.

Added

- ARGO-1365 Add config noreplace param in spec file
- ARGO-1364 Set-cap option in spec file
- ARGO-1122 Subscriptions - Set default functionality for pulling messages to return immediately
- ARGO-1279 API CALL - Health check
- ARGO-1307 Update ams service file to include a syslog identifier
- ARGO-1307 Update ams service file to include a syslog identifier
- ARGO-1281 Add support for logging to syslog
- ARGO-571 Use const for error messages in messaging service
- ARGO-1085 Add info on Ack timeout error for argo-messaging service
- ARGO-1154 API CALL - Return User given a UUID
- ARGO-1158 Expose UUID field when querying users
- ARGO-1157 Add get user by Token

Changed

- ARGO-1359 Handle empty project_uuid references
- ARGO-1216 Retry if backends are unavailable

Fixed

- ARGO-1282 Fix Metrics package timestamp to be utc
- ARGO-1003 Fix publishedTime to be in UTC instead of localtime
- ARGO-1177 Fix utc generation in utc-formatted fields

Releases

v1.0.3-1 - https://github.com/ARGOeu/argo-messaging/releases/tag/1.0.3-1 - 31 July 2018

v1.0.2 - https://github.com/ARGOeu/argo-messaging/releases/tag/1.0.2 - 7 June 2018

5.5.2.2 argo-ams-library

A simple library to interact with the ARGO Messaging Service.

Fixed

- Error handling bug during list_topic route and upgrade to v0.4.2
- Fix returnImmediately parameter in sub pull request

Added

- Tests for backend error messages that could be plaintext or JSON encoded
- Extend AMS client to support X509 method via the authentication
- Extend ams library to support offset manipulation
- Introduce AmsHttpRequests class
- Extend ams library to support offset manipulation
- Grab methods from class namespace
- Tests for bogus offset specified
- Added missed 'all' value for offset argument
- Handle 404 for topic and subscription calls
- Handle JSON error message propagated through AMS
- set for error codes and pass request args for iters
- Status msg attach to AmsServiceException if exist
- Topic ALREADY_EXIST error test
- Remove not raised TypeError exception handles
- Offsets method with combined logic of get and move offsets

Changed:

- Updated error handling
- Common methods for PUT, GET, POST requests
- Failed TopicPublish and CreateSubscription tests
- Separated error mocks
- Refactored error handling with error routes

Available Releases

- Version 0.4.2-1 - 26July 2018 - https://github.com/ARGOeu/argo-ams-library/releases/tag/v0.4.2
- Version 0.4.0-1 - 9 May 2018 - https://github.com/ARGOeu/argo-ams-library/releases/tag/v0.4.0-1

5.5.2.3 *Argo-AuthN*

Argo-authn is a new Authentication Service. This service provides the ability to different services to use alternative authentication mechanisms without having to store additional user info or implement new functionalities.The AUTH service holds various information about a service's users, hosts, API urls, etc, and leverages them to provide its functionality.

Added

- ARGO-1168 Auth Service Initialisation
- ARGO-1171 Database Interface with some basic functionality
- ARGO-1172 Add functionality for required struct tags and convert structure
- ARGO-1173 Generic Handlers and Routing
- ARGO-1174 API CALL - Create Service
- ARGO-1176 API CALL - Get service(s)
- ARGO-1183 API CALL - Get Auth method(s)
- ARGO-1182 API CALL - Create Auth method
- ARGO-1184 API AuthN: Service types - use uuid
- ARGO-1205 API AuthN: Authentication method - use uuid
- ARGO-1211 API CALL - Create Binding
- ARGO-1212 API CALL - Get binding(s)
- ARGO-1222 List all auth methods bug fix
- ARGO-1123 List all service types bug fix
- ARGO-1165 X509 API Call
- ARGO-1121 Script for creating users

- ARGO-1213 API CALL - Update Binding
- ARGO-1248 - create argo-api spec file
- ARGO-1214 API CALL - Delete Binding
- ARGO-1124 Better documentation and errors for argo-authN service types
- ARGO-1189 API Call - Update Service Type
- ARGO-1191 API CALL - Delete Auth Method
- ARGO-1191 API CALL - Delete Auth Method
- ARGO-1272 Extend RDNSequence to string method to support DC rdn
- ARGO-1254 Service build and management fixes
- ARGO-1237 Add SysLogHandler
- ARGO-1280 Check Revocation List
- ARGO-1283 Check certificate expiration date
- ARGO-1284 Certificate verify hostname
- ARGO-1306 Update authn service file to include syslog name
- ARGO-1293 Deprecate existing auth_methods package and its uses
- ARGO-1280 Check Revocation List
- ARGO-1283 Check certificate expiration date
- ARGO-1293 Deprecate existing auth_methods package and its uses
- ARGO-1312 Add utils method that sets a value to field given its name
- ARGO-1206 API CALL - Update Auth method
- ARGO-1323 Ability to set up the service without cert verification
- ARGO-1190 API CALL - Delete Service-type
- ARGO-1362 Database Session Clone functionality

Removed

- ARGO-1297 Remove deprecated package auth_methods and its uses

Changed

- ARGO-1363 Check for unsupported auth type for the service type
- ARGO-1227 Refactor Create Binding to also assign a UUID
- ARGO-1228 Refactor Get Binding(s) to work with UUID
- ARGO-1220 Refactor errors to not expose go struct info
- ARGO-1301 Refactor service-type - Add an additional field named type
- ARGO-1304 Refactor service-types - remove field retrieval field
- ARGO-1300 Refactor x509 mapping to use the new auth method interface
- ARGO-1301 Refactor service-type - Add an additional field named type
- ARGO-1294 Refactor Create auth method using structs
- ARGO-1295 Refactor Get auth method(s) using structs
- ARGO-1305 Refactor datastore to deal with the new version of auth methods
- ARGO-1311 Refactor utils method GetFieldValueByName
- ARGO-1301 Refactor service-type - Add an additional field named type

5.5.3 Future plans

- Support, maintain, extend the AMS Service
- Support, maintain, extend the AuthN Service
- Support FedCloud Information System
- Support AppDB

5.6 Security Tools

5.6.1 Pakiti

5.6.1.1 Overview

Service/Tool name	Pakiti
Service/Tool url	https://github.com/CESNET/pakiti-server https://github.com/CESNET/pakiti-client
Service/Tool information page	https://pakiti.egi.eu/ https://pakiti.cesnet.cz/egi/
Description	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.
Value proposition	Proper security patch management is a crucial service to achieve a secure environment, yet it often is not straightforward to implement reliably. Pakiti detects missing security updates and notifies security teams and/or administrators so the vulnerabilities can be fixed before they cause security incidents.
Customer of the service/tool	RI; Resource Provider; NGIs
User of the service/tool	Site admins; Operations Managers; security teams of sites and infrastructures
User Documentation	https://github.com/CESNET/pakiti-server/tree/master/docs
Technical Documentation	https://github.com/CESNET/pakiti-server/tree/master/docs
Product team	CESNET
License	BSD 2-Clause
Source code	https://github.com/CESNET/pakiti-server https://github.com/CESNET/pakiti-client

Testing	manually-controlled checks focused on handling typical tasks.

5.6.1.2 Release notes

5.6.1.2.1 Pakiti server

Pakiti server releases are available from GitHub [R14].

2018-11-04

Changed

- doc: Fix DSA URL, add Ubuntu Bionic

2018-10-18

Changed

- Remove all the passing Objects around by reference in function calls and in foreach loops. They are unnecessary for objects and generate PHP Notices in PHP > 7.0.7

2018-09-20

Added

- Add next debian and current Ubuntu LTS to config template OS group mapping

Changed

- Update README.md

2018-09-19

Changed

- Remove eval() from codebase. We can create the required objects directly rather than use eval().
- Improve handling of client parameters

2018-09-17

Changed

- Add a scope qualifier to the variable
- Add a basic message when access is forbidden
- Don't add vulnerability definitions for unknown OS Groups. (v2)
- Add the right link to host packages

2018-09-04

Changed

- Improve descriptions on the title page

2018-09-03

Fixed

- Fix invalid links to host_cves.php and host_reports.php

2018-08-31

Changed

- Update configuration.md
- Prepend string "Pakiti" to all log records

- Use the right constant name when logging errors

2018-08-20

Fixed

- Calculate correctly the length of fake kernel release.

2018-08-03

Changed

- Improve handling of kernel packages on storing.
- Don't add vulnerability definitions for unknown OS Groups.

2018-08-02

Changed

- Make the test IGNORE_PACKAGES_PATTERNS really work.
- Treat IGNORE_PACKAGES_PATTERNS and IGNORE_PACKAGES equally.

2018-08-01

Changed

- Enable '=' as the delimiter of CLI parameters.

2018-07-31

Fixed

- Handle the config option properly

2018-07-17

Changed

- Adapt package installation
- Adapt file paths.
- Use utf8 as the default encoding for Pakiti DB.

2018-07-16

Changed

- Revise the output of Feeder
- Log messages are sent to stderr only from CLI context
- return gracefully from the script

2018-07-11

Changed

- Support a new way of getting information on Debian vulnerabilities.

2018-01-20

Changed

- Proper handling of multiple kernel packages on Debian installations
- Improve logging messages.

2018-01-19

Added

- Support the config command-line option

Changed

- More resilient args parsing in the helper library.

2018-01-17

Added

- Add support for CentOS versioning.

Changed

- Refactor the SubSource classes, utilizing inheritance to a larger extent.

2018-01-16

Fixed

- Fixed population of OsGroups

2018-01-15

Added

- Extended functions of the hosts.php CLI tool.

5.6.1.2.2 Pakiti client

Pakit client releases are available from GitHub [R15].

2018-11-06

Changed

- Move the client script to the top-level directory.
- Review the communication protocol to unify handling of HTTP responses.

2018-07-18

Added

- Added support for SVMON on pakiti.

2018-07-13

Changed

- Read the OS also from /etc/os-release

2018-05-22

Changed

- Simplify RPM packaging

5.6.1.3 Future plans

- Support of integration with SVMON
- Evaluation of the deployment for EGI CSIRT
- Support and maintenance

5.6.2 Secant

5.6.2.1 Overview

Service/Tool name	Secant
Service/Tool url	https://github.com/CESNET/secant
Service/Tool information page	https://github.com/CESNET/secant
Description	Secant is a security cloud assessment framework that is used to check 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 error or vulnerabilities commonly misused by Internet attackers.
Value proposition	Security of IaaS is largely determined by the running virtual clouds so it is crucial the images used for their instantiation are securely configured. Secant makes it possible to reveal common errors and ease the maintenance of cloud images.
Customer of the service/tool	RI; Cloud Resource Provider; Communities
User of the service/tool	Site admins; Operations Managers; security teams of sites and infrastructures
User Documentation	https://github.com/CESNET/secant
Technical Documentation	https://github.com/CESNET/secant
Product team	CESNET
License	Apache License 2.0
Source code	https://github.com/CESNET/secant
Testing	manually-controlled checks focused on handling typical tasks.

*5.6.2.2 **Release notes***

No fixed release was published, the running instance is based on rolling updates. Changes delivered since the start of the project:

Changed

- Code improvements and bug fixes
    - improved logging
    - improved utility and usability of auxiliary scripts
    - OpenNebula control was moved to a single file
    - VM contextualization reworked
    - improved control of VM life-cycle
- Probes improvements
    - existing probes made more robust
    - probes can consume results of other probes
    - new probes added (weak SSH passwords)
    - new structure of probes, allowing easy development of new ones
    - status codes unified
- Documentation updated
- Configuration extended
    - new directives introduced
    - a separate configuration file for probes

Added

- Support for checking the status of contextualization progress
- Added locks to prevent from potential conflicts
- Reviewed output format for AppDB (adding message id and additional fields)
- Robust integration with cloud-keeper
- Improved management of artifacts after analysis

5.6.2.3 Future plans

- Support and maintenance
- Evaluation of integration with AppDB

6 Helpdesk Services and Tools

6.1 Overview

This chapter provides the release notes and the future plans for the EOSC-hub helpdesk services and tools.

GGUS is the central helpdesk service for the EGI, WLCG e-Infrastructures and more than 40 other Virtual Organisations. It is synchronized with 16 other grid related helpdesk systems and interfaced with existing EGI tools like the GOCDB or the Operations Portal to exchange system relevant information.

The EUDAT Trouble Ticketing System (TTS) provides the 1st and the 2nd level support for all the EUDAT services. The different levels of support are managed by dedicated teams. The TTS system is currently including more than 41 teams managing different queues.

The unified ticketing system used for EOSC-hub project will be xGUS, a developed lightweight clone of GGUS that permits a basic level of interoperability with GGUS and RT. The unified ticketing system will provide a central place for managing the 1st level support tickets for all users independently of the final service/infrastructure being used.

6.2 GGUS

6.2.1 Overview

Service/Tool name	GGUS
Service/Tool url	https://ggus.eu
Service/Tool information page	https://wiki.egi.eu/wiki/GGUS
Description	GGUS helpdesk is a single point of contact for all EGI customers for requesting help for fixing issues.
Value proposition	Besides WLCG GGUS covers a wide range of VOs and tool developers providing user support for their customers. It is connected to various ticketing systems of NGIs and infrastructures e.g. in the US.
Customer of the service/tool	EGI customers
User of the service/tool	Service providers, site admins, operations
User Documentation	https://ggus.eu/?mode=docu
Technical Documentation	https://wiki.egi.eu/wiki/GGUS

Product team	KIT
License	BMC Remedy (Closed source)
Source code	n.a.
Testing	https://test.ggus.eu/ggus/?mode=index

6.2.2 Release notes

2018-11-28

Security

- installed security updates and patches

2018-09-26

Added

- new ticket categories "Release" and "CMS Internal"

Removed

- removed support unit EGI Cloud Data Management

Security

- installed security updates and patches

2018-07-25

Added

- support units "EGI Notebooks", "EGI DataHub", "EGI DataTransfer"

Removed

- removed support unit NGI_INDIA

Security

- installed security updates and patches

2018-05-16

Added

- new support unit “OSG Software Support”

Removed

- removed support units: LSF Utils and SGE Utils
- removed VO "vo.elixir-europe.org"

Security

- installed security updates and patches

2018-01-31

Added

- anonymisation of user data
- keep external ticket IDs in the subject of emails
- for tickets to multiple sites allow ticket creation on behalf of a support unit
- distinction between ticket under EGI and WLCG responsibility

Changed

- improved site selection for tickets to multiple sites

Security

- installed security updates and patches

6.2.3 Future plans

All GGUS instances (development, pre-production and production) are maintained on a regular basis. During the maintenance window, system updates and security patches are installed and the system can be equipped with requested and approved features. New requirements for the improvement of the service are tracked in [R16], [R17].

6.3 EUDAT-RT

6.3.1 Overview

Service/Tool name	EUDAT-RT
Service/Tool url	https://helpdesk.eudat.eu
Service/Tool information page	https://confluence.csc.fi/pages/viewpage.action?pageId=50874303
Description	EUDAT-RT is the ticketing system used for EUDAT-CDI to manage the first level and 2nd level support request for all its services. The EUDAT-RT service is based in the Request Tracker software and it includes several support units to manage all the services of the EUDAT infrastructure.
Value proposition	The EUDAT-RT service is the main entry point for requests, problems and incidents for the EUDAT infrastructure. The service supports federated access through B2ACCESS and it is used by all the EUDAT staff and EUDAT users to submit and keep track of the problems concerning EUDAT services. EUDAT-RT will be linked with the current EOSC-hub helpdesk system, based on xGUS, this integration will permit the management of tickets received on xGUS and assigned to EUDAT infrastructure. Any update on tickets generated on xGUS and migrated to EUDAT-RT will be automatically propagated to xGUS in order to have a full history of all the tickets on the xGUS TTS.
Customer of the service/tool	Research Communities, any user of EUDAT services.
User of the service/tool	Support units and 1st level support team of EUDAT.

User Documentation	https://confluence.csc.fi/download/attachments/50865867/eudat-TTS-Manual_2017v1.pdf?version=1&modificationDate=1502872233908&api=v2
Technical Documentation	https://confluence.csc.fi/pages/viewpage.action?pageId=50874303
Product team	BSC-CNS
License	RT- Request tracker from Best Practical - Version 2 of the GNU General Public *License*
Source code	https://bestpractical.com/download-page
Testing	Deploying a new version of the service requires tests for the following functions: • creation of tickets • movement and assignation of tickets to the different support units (queues) • generation of e-mails from the system (send/recv) • access to the system through B2ACCESS • recovering of all the previous tickets and status (full RT DataBase comprovation)

6.3.2 Release notes

1.0.0 - 2018-11-19

Changed

- First release after the migration of the service from CINECA to BSC

Added

- Support for B2ACCESS authentication

6.3.3 Future plans

- Improve the integration between xGUS and EUDAT-RT: While, currently, the 2 ticketing systems communicate via emails, the end goal is to use the SOAP interface available on xGUS to communicate any change between the ticketing systems (changes in answers, ticket status, priority, etc).

6.4 xGUS

6.4.1 Overview

Service/Tool name	EOSC-hub helpdesk
Service/Tool url	https://helpdesk.eosc-hub.eu

Service/Tool information page	https://confluence.egi.eu/display/EOSC/xGUS
Description	EOSC-hub helpdesk is a single point of contact for all EOSC customers for requesting help for fixing issues.
Value proposition	EOSC customers do not need to know which infrastructure an issue is related to. They can submit their ticket in EOSC-hub helpdesk. It will be routed to the appropriate instances for fixing it.
Customer of the service/tool	EOSC-hub customers
User of the service/tool	Service providers, site admins, operations
User Documentation	n.a.
Technical Documentation	n.a.
Product team	KIT
License	BMC Remedy (Closed source)
Source code	n.a.
Testing	n.a.

6.4.2 Release notes

1.0.0 - 2018-10-26

Changed

- First version
- Integration with EGI SSO
- Full synchronization with GGUS
- Integration with EUDAT RT based on email and manual interaction

6.4.3 Future plans

- Implement SOAP interface for full automatic integration with EUDAT RT

7 Application store, Software Repositories and other Collaboration Tools

7.1 Overview

In this chapter, release notes and future plans about the following services will be provided:

The **Applications Database** (AppDB) is a central service that stores and provides to the public information about:

- software solutions in the form of native software products and virtual or software appliances,
- the programmers and the scientists who are involved, and
- publications derived from the registered solutions.

In addition, AppDB is the responsible unit within the EOSC-hub ecosystem, for:

- distributing the registered VM images to the resource providers and
- enabling users to deploy and manage Virtual Machines to the EGI Cloud infrastructure through AppDB's dashboard services

GitLab is a web-based platform, which provides an integrated environment for software development including Git-repository, issue tracking system, wiki, continuous integration module etc. GitLab is used as integrated solution for full software development cycle and provides rich APIs for integration with other services. Fully automated workflows for software testing and deployment implemented in GitLab can be used for efficient release and deployment management for EOSC-hub distributed services. GitLab instance deployed at KIT is integrated with Container Registry [R18], which allows storing Docker images. The federated access to the GItLab is provided by the EUDAT AAI solution B2ACCESS, thus GitLab resources and Git-repositories are available for many research communities and scientific organizations.

The **EGI Software Repository** implements all necessary management workflows for the UMD & CMD Middleware Distributions and the Community Software, while providing a unified point of access to these resources, which are described below:

- the Unified Middleware Distribution (UMD) is the integrated set of software components contributed by Technology Providers and packaged for deployment as production quality services in EOSC-hub.
- the Cloud Middleware Distribution (CMD) distributes OpenStack and OpenNebula integration components, developed by Cloud Technology Providers. Two different distributions are technically available, CMD-OS for OpenStack and CMD-ONE for OpenNebula.
- the Community Software is strongly integrated with the AppDB system and consists of repositories of binary artifacts, provided by communities and individuals affiliated with the EOSC-hub project.

7.2 Applications Database

7.2.1 Overview

Service/Tool name	EGI Applications Database (AppDB)

Service/Tool url	https://appdb.egi.eu/
Service/Tool information page	https://wiki.egi.eu/wiki/AppDB
Description	The EGI Applications Database (AppDB) is a central service that stores and provides to the public information about: • **software solutions** in the form of **native software products** and/or **virtual appliances**, • the **programmers** and the **scientists** who are involved, and • **publications** derived from the registered solutions • enabling users to **deploy** and **manage Virtual Machines** to the EGI Cloud infrastructure through the VMOps Dashboard [R19] Reusing software products, registered in the AppDB, means that scientists and developers may find a solution that can be directly utilized on the European Grid & Cloud Infrastructures without reinventing the wheel. This way, scientists can spend less or even no time developing, porting or even using a software solution to the Distributed Computing Infrastructures (DCIs). AppDB, thus, aims to avoid duplication of effort across the DCI communities, and to inspire scientists less familiar with DCI programming and usage.
Value proposition	• Users can promote their software solutions and resources, reaching a large audience of peers, by registering them and describing them in a dedicated central database • Users can reach a larger audience outside their peers, by having information related to their software solution propagated to other third-party services e.g. Resource Providers, ARGO, OpenAIRE, through interservice integration via its web-API • Users gain a medium of directly interacting with the computing infrastructure in a graphical way.
Customer of the service/tool	RI; Resource Providers; Research Communities;
User of the service/tool	Site admins; Operations Managers; large research groups; Individual researchers
User Documentation	https://wiki.appdb.egi.eu/
Technical Documentation	https://wiki.appdb.egi.eu/
Product team	IASA
License	Apache License Version 2.0

Source code	https://github.com/iasa-gr
Testing	Unit & functional tests performed on the AppDB development instance [R20].

7.2.2 Release notes

The EGI Applications Database is constituted by a number of sub-services, each of which follows different versioning, thus different release cycle and therefore their release notes are provided separately. The following sub-services are those that present significant activity within the reporting period:

7.2.2.1 AppDB portal

6.1.10 - 2018-09-11

Added

- Import publication information for software and vappliance in various formats (biblatex, bib, copac, ebi, end, endx, isi, med, nbib, ris, wordbib)

Changed

- Pass extended account information to authorized sub services (vmops dashboard)
- Replace php file_get_contents with cURL
- Improved support for OpenAIRE project and organization metadata synchronization

Fixed

- Invalid dojo versioning report due to custom build
- Fixed bug causing empty category and discipline collections when creating new software and vappliance entries

6.1.9 - 2018-08-30

Fixed

- Properly display secant multiline details

6.1.8 - 2018-08-29

Added

- Added vomses information regarding geohazards.terradue.com, hydrology.terradue.com, vo.geoss.eu
- Funded by relation support for sw/va and projects

Changed

- Revised UI of VO wide image list editor
- Display secant backend service outcome in security report UI
- Set software last updated date when performing software repository actions
- Update countries information
- Update vomses information
- Performance improvements when saving software and vappliance items

Fixed

- Fixed bug rendering empty history list of edits for software and vappliance items
- Fixed bug causing predefined middlewares of software items to be saved as custom middlewares

6.1.7 - 2018-07-02

Changed

- Improve performance by performing asynchronous calls to DB where possible
- Performance improvements when generating software, vappliance, person and permissions XML

Fixed

- Avoid cache race conditions in filter items function
- Define xmlns:xsi namespace on elements that make use of xsi:nil to avoid XML errors inside the database
- Avoid possible null array references in REST API causing unhandled exceptions
- Ensure all related DB entries are refreshed on software and vappliance updates (permissions etc)
- use view for application hitcount in ARO model
- Fix relation type literals in DB

6.1.6 - 2018-06-27

Changed

- Allow only administrators to register new user profiles from UI (removed managers)
- People profile searching returns more relative results

Fixed

- Fixed profile validation mechanism when a new user registers

6.1.5 - 2018-06-22

Security

- Migrate jQuery to version 3.x
- Removed dead code

Fixed

- Fix binary artifact types to recognize tar and gz formats in software repository

6.1.4 - 2018-06-08

Fixed

- Properly handle secant's failed checks due to internal failure

6.1.3 - 2018-05-24

Changed

- Group sequential log entries and display count in continuous delivery view
- Bug fixes and improvements
- Clean up automatic mail subscriptions that the user did not opt in (GDPR related)
- Disable notifications for outdated applications (GDPR related)
- Make profile contact information and VO membership available only to the same user account (GDPR related)

Security

- Differentiate handling of REST api calls from AppDBs client code and external calls in order to avoid external malicious javascript code to be executed on behalf of the logged in user

Removed

- Export button from people list (GDPR related)
- Broken links report as it lacked accuracy and code became obsolete

Fixed

- Various bugs regarding the atom news feed
- Respond with tag information when inserting a new tag on sofwtare and vappliance
- Properly identify users access groups when accessing REST api using access token

6.1.2 - 2018-05-14

Added

- Integration with virtual appliance continuous delivery sub service

Removed

- Removed gender information from person profile (GDPR related)

6.1.1 - 2018-05-02

Added

- PID related support to software and vappliance entries
- Support for diffs of software and vappliance change history in UI and REST api

Changed

- Conform with EGI AAI entitlements format changes
- Retrieve site contact information from EGI AAI entitlements
- Replace links to vmcatcher with CloudKeeper

Fixed

- Display message when an entry was not found due to invalid url

6.1.0 - 2018-03-26

Added

- Integration with secant service
- Added biomed and enmr.eu VOMS related files in public ui assets

7.2.2.2 VMOps dashboard

1.2.0 - 2018-10-23

Added

- Partial loading of resources in client when needed

Changed

- Modularize codebase to accept (enable/disable) new features/dashboards

1.1.2 - 2018-09-25

Changed

- Version update of package dependencies

Fixed

- Fix data binding of current item and its derived UI modals

1.1.1 - 2018-09-14

Added

- Support for VO vo.geoss.eu and VO vo.emsodev.eu

Fixed

- Fix handling of empty account display name
- Various bug fixes and code improvements

1.1.0 - 2018-07-04

Added

- Enable users to explicitly request if the topology VMs will have public ips during topology configuration. Defaults to true.
- Enable users to request for a new public IP or remove an existing public IP in running VMs.
- Enable users to create and attach new block storages in running VMs.
- Support for VO beapps, geohazards.terradue.com and hydrology.terradue.com

Fixed

- Handle edge cases where topologies are in a failed state but already acquired resources (VMs, block storages, public IPs etc)

1.0.0 - 05-03-2018

Added

- Support EGI VM Operations with EGI AAI Authorization

7.2.2.3 VMOps service

1.5.5 - 2018-10-25

Fixed

- Do not monitor topologies in an unknown state if they where previously undeployed by the infrastructure

1.5.4 - 2018-09-25

Fixed

- Not retrieving tickets from non existing topology

1.5.3 - 2018-09-14

Added

- Pass server time in sync operations for helping clients calculate time spans of operations

1.5.2 - 2018-07-09

Fixed

- Ensure the tasks monitoring active,running and stopped topologies do not overlap unknown topologies monitor task
- Properly set production related environment variables
- Stop updating state change date field on each sync if infrastructure state is not changed

1.5.1 - 2018-06-29

Fixed

- Fix detection of public IP creation/removal action is complete

1.5.0 - 2018-06-07

Added

- Funcional request mechanism for requesting new public IP or remove existing one for deployed VMs

Fixed

- Properly set network section of topology data upon update
- Do not save topology network meta data that do not correspond to existing VM networks during sync process.

1.4.0 - 2018-05-31

Added

- Funcional request mechanism for creating and attaching new block storages to deployed VMs

Changed

- Generate proper RADL for requesting a new block storage from IM

Fixed

- Better detect if a block storage action is completed
- Properly pass parameters to PUT request to IM rest API

1.3.3 - 2018-05-23

Fixed

- Update date of state change of a topology/VM only if infrastructure state value have changed
- Immediately set topology to stopped if all VMs are stopped, instead of waiting the next sync process

1.3.2 - 2018-05-22

Added

- Initial implementation to request new block storages for already deployed VMs

Fixed

- Do not set topology in failed state if has initialized resources. Must be undeployed first to release them

1.3.1 - 2018-03-19

Added

- Bash scripts to produce daily reports for last day, last number of months and last year

Fixed

- Better deduce if an action is a failed one during daily report building
- Fix data inconsistencies in daily report building

1.3.0 - 2018-03-16

Added

- Generate daily reports for activity of topologies and VMs managed by the VMOPs service

1.2.0 - 2018-02-01

Added

- Ticket manager to store and provide external opened tickets regarding specific topologies and VMs

*7.2.2.4 **InfoSys publisher***

1.3.1 - 2018-04-23

Changed

- Code revision and documentation
- Revised logging information

1.3.0 - 2018-01-16

Added

- Add WARNING in site service status enumeration
- Add enumeration filtering in REST API
- Add argo status and gocdb downtime in site and service details for REST API
- Add argo service statuses resource in REST API
- Add gocdb downtimes resource in REST API

Changed

- Update apollo-server dependency package to v1.3.2

Fixed

- Fix relation of service statuses to site services in entity model

7.2.2.5 ***InfoSys MsgQ Listener***

0.2.0 - 2018-10-31

Added

- Central logging mechanism

Changed

- Handle and log SIGINTs events
- Update dependencies versions

Removed

- PM2 logging configuration

0.1.2 - 2018-10-23

Added

- Configure PM2 service to log to files
- Configuration for maximum subscription items of ArgoMQ module

Changed

- Reduced logging information

Fixed

- Properly parse subscription response to avoid raising invalid events

0.1.1 - 2018-10-18

Added

- Configurable auto acknowledge for ArgoMQ subscriptions

Changed

- Provide more generalized default configuration file
- Do not proceed with saving information if subscription empty is empty
- Revised log entries

Fixed

- Decode base64 subscription messages to utf8 instead of decoding it to buffer object.
- Remove possible debug annotations from LDIF messages

7.2.3 Future plans

- Provide support for OpenID Connect
- Extend the AppDB IS to support GLUE 2.1 schema
- Development of the Endorser Dashboard
- VMOps dashboard: drop OCCI – provide support of native APIs
- VMOps dashboard: provide support about VO user based quotas for cloud resources

7.3 GitLab

7.3.1 Overview

Service/Tool name	GitLab
Service/Tool url	https://gitlab.eudat.eu
Service/Tool information page	https://about.gitlab.com/
Description	GitLab is the first single application for the entire DevOps lifecycle.
Value proposition	GitLab provides an integrated environment for software development and continuous integration.
Customer of the service/tool	EOSC-hub customers
User of the service/tool	Research communities, individual researchers, service providers.
User Documentation	https://docs.gitlab.com/
Technical Documentation	https://docs.gitlab.com/
Product team	KIT
License	MIT License
Source code	https://gitlab.com/gitlab-org/gitlab-ce
Testing	functions test (webview, api)

7.3.2 Release notes

1.2.7 - 2018-11-05:

Changed

- Update Gitlab to version 11.4.5

1.2.6 - 2018-10-05:

Changed

- Update Gitlab to version 11.3.5

1.2.5 - 2018-08-23:

Changed

- Update Gitlab to version 11.2.1

1.2.4 - 2018-07-31:

Changed

- Update Gitlab to version 11.1.4

1.2.3 - 2018-07-12

Changed

- Update B2ACCESS SAML idp_cert

1.2.2- 2018-07-05:

Changed

- Update Gitlab to version 11.0.3

1.2.1 - 2018-05-22:

Changed

- Update Gitlab to version 10.7.4

1.2.0 - 2018-05-18

Added

- Support GitLab Large File Storage (LFS)

1.1.1 - 2018-04-09:

Changed

- Update Gitlab to version 10.6.4

1.1.0 - 2018-03-16

Added

- Support OAuth2.0 provider feature, connect with mattermost service

1.0.2- 2018-03-09:

Changed

- Update Gitlab to version 10.5.4

1.0.1- 2018-02-16

Changed

- Update Gitlab to version 10.4.4

1.0.0 - 2018-01-02

Changed

- First release: Gitlab version 10.3.3

7.3.3 Future plans

- Support GitLab Continuous Integration & Deployment (CI/CD)
- Integrate with AppDB (https://appdb.egi.eu/)

7.4 EGI software repository

7.4.1 7.4.1 Overview

Service/Tool name	EGI Software Repository
Service/Tool url	http://repository.egi.eu/
Service/Tool information page	http://repository.egi.eu/about
Description	The EGI Software Repository ecosystem is a collection of services for supporting the management and the provisioning of the software artifacts that compose the **UMD** (Unified Middleware Distribution) and the **CMD** (Cloud Middleware Distribution), the **Community Repositories**, and the operational tools developed by the consortium. The following sub-services are included: • Repository back-end • Repository front-end • Composer • UMD, CMD & Community repositories The Repository back-end and the Composer services, are the units within the EGI Software Repository ecosystem that are responsible for the construction of UMD and CMD releases and their related repositories. The Repository front-end is for making the produced repositories and all the required information, available to the public. Finally, the EGI Software repository is strongly integrated with the Application Database (AppDB). In this case, the AppDB acts as the backend “engine” for creating and managing the Community repositories populated through the EGI Software Repository system.

Value proposition	The EGI Software provisioning infrastructure (including RT) supports technology providers on their effort in delivering releases with respect to their products. From the other end, the provisioning infrastructure is responsible for supporting the verification of submitted releases, from a quality perspective, and for delivering ready-to-use repositories to the end-users, i.e. site admins, operation managers, and research communities.
Customer of the service/tool	RI; Resource Provider; Research Communities
User of the service/tool	Site admins; Operations Managers; large research group
User Documentation	http://repository.egi.eu/category/umd_releases/distribution/umd-4/ http://repository.egi.eu/category/os-distribution/cmd-os-1/ http://repository.egi.eu/category/one-distribution/cmd-one-1/
Technical Documentation	https://wiki.egi.eu/wiki/EGI_Software_Provisioning https://wiki.egi.eu/wiki/Middleware https://wiki.egi.eu/wiki/EGI_Cloud_Middleware_Distribution
Product team	IASA
License	Apache License Version 2.0
Source code	https://trac.iasa.gr/trac/egi-repo/
Testing	Unit and integration tests are part of development and deployment process. The code review is a part of the development process. In addition there is a dedicated flow, under which, changes in the code that will potentially affect the smooth operation of the EGI repository are tested in a fully operational environment prior they are committed to the master branch and therefore pushed into production.

7.4.2 Release notes

2.0.6 - 2018-08-29

Changed

- Extend the logging facility of the Software provisioning infrastructure

Added

- Deploy & further develop a tool for providing statistical info from the collected logs

2.0.5 - 2018-07-25

Changed

- Migration of the administration instance of the EGI Repository frontend to a new virtualized infrastructure provided by the institute
- Upgrade the RPM based agent, responsible unit for building the YUM repositories

2.0.4 - 2018-05-07

Changed

- Several fixes to the RSS/REST API that provides data from the backend to the frontend
- Performance improvements

7.4.3 Future plans

The following ideas are currently under evaluation:

- Integration of Jenkins Continuous Integration (CI) with the EGI software repository
- Using the AppDB portal as the front-end for the EGI software repository

References

No	*Description/Link*
R1	https://www.eosc-hub.eu/catalogue
R2	https://keepachangelog.com
R3	https://aarc-project.eu/guidelines/aarc-g002/
R4	https://rcauth.eu/policy/
R5	https://confluence.egi.eu/display/EOSC/5.3.2
R6	https://confluence.egi.eu/display/EOSC/5.2.2
R7	https://plone.org/
R8	https://github.com/EUDAT-DPMT/pcp.contenttypes
R9	https://pypi.org/project/plone.restapi/
R10	https://github.com/hmpf/easydmp/blob/master/CHANGELOG.rst
R11	https://github.com/postmanlabs/newman
R12	https://getpostman.com
R13	https://www.getpostman.com/docs/collections
R14	https://github.com/CESNET/pakiti-server/releases
R15	https://github.com/CESNET/pakiti-client/releases
R16	https://rt.egi.eu/rt/Dashboards/2636/GGUS-Requirements
R17	https://its.cern.ch/jira/browse/GGUS
R18	https://about.gitlab.com/2016/05/23/gitlab-container-registry/
R19	https://dashboard.appdb.egi.eu
R20	https://appdb-dev.marie.hellasgrid.gr/