D5.4 Second release of federation and collaboration services and tools

Lead Partner:	KIT
Version:	1
Status:	FINAL
Dissemination Level:	Public
Document Link:	https://documents.egi.eu/document/3561

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 second 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 and also included in WP5 roadmap, provided at the end of the document.

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

COPYRIGHT NOTICE

DELIVERY SLIP

Date	***Name***	***Partner/Activity***	***Date***
From:	Pavel Weber	WP5/KIT	
Moderated by:	Malgorzata Krakowian	WP1/EGI	
Reviewed by:	John Alan Kennedy Giacinto Donvito	WP6/KIT WP10/INFN	2020-02-15
Approved by:	AMB		

DOCUMENT LOG

Issue	***Date***	***Comment***	***Author***
v.0.1	2019-09-02	Finalised table of contents	Pavel Weber
v.0.2	2019-10-20	All contributions for sections/tools provided	Nicolas Liampotis Kostas Koumantaros Themis Zamani William V. Karageorgos Adrian Coveney Cyril L'orphelin Pavel Weber Marcus Hardt Alexandros Nakos Ivan Diaz Alvarez Jens Jensen Greg Corbett Raphael Ritz Daniel Kouril Christos Kanellopoulos Sander Apweiler Mischa Salle Slavik Licehammer Enrico Vianello Agnieszka Pulapa
v.0.3	2019-11-15	Added executive summary	Pavel Weber
v.0.4	2019-11-20	Added glossary	Pavel Weber
v.0.5	2020-01-16	Ready for external review	Pavel Weber
v.0.6	2020-02-14	Comments added by external reviewers	Pavel Weber

v.1.0	2020-02-25	Final version	Pavel Weber

TERMINOLOGY

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

Terminology/Acronym	*Definition*
AAI	Authorization and Authentication Infrastructure
AARC	Authentication and Authorisation for Research and Collaboration
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.

The federation and collaboration services are the components of the EOSC-hub Key Exploitable Results (KER) “Internal Services Provided in the Hub Portfolio” and “EOSC Portal and Marketplace”.

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 second year of the project. These changes have been prepared and agreed among the WP5 partners and EOSC-hub technical coordination group (WP10).

1 Introduction

The short 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 contains a set of subsections 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].

Finally, the roadmap for the whole WP5 is given at the end of the document and contains the list of tasks for each service with preliminary due dates.

2 Identification, Authentication, Authorisation and Attribute Management

2.1 B2ACCESS

2.1.1 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-2.8.2/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

[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.

	are done by operators, 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.
TRL	9

2.1.2 Release notes

11.12.2019:

- Update of the underlying software.
- Enhancement of group management: Enabling a new endpoint for managing group membership by the group administrators itself. Previously the group management must be handled by the service operators.
- Update of the layout: The look of the remote identity provider presentation was updated to a modern layout and the colour scheme was updated.
- Enhancement of user login: Remembrance of users last used identity provider to simplify and speedup the re-login to the service.

2.1.3 Future plans

- Harmonisation of AUP
- Update of underlying software stack

2.2 Check-in

2.2.1 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.
TRL	9

2.2.2 Release notes

Unreleased
Added

- Add support for parametric scopes: Parametric scopes can be used to filter the returned claim values when requesting a given scope in its parametric form. The syntax of the parametric scope is: `<scope_name><delimiter><scope_parameter>`
- Add support for Proof Key for Code Exchange (PKCE): PKCE is a technique for securing public clients that don't use a client secret (https://tools.ietf.org/html/rfc7636)
- Add support for redirecting the user to the end service they were trying to access after completing the user registration process

v19.10.1 - 2019-10-11

Fixed

- Fixed group search functionality in Group Management UI which was breaking in debug mode due to undefined/missing variable

v19.09.3 - 2019-09-20

Added

- Add support for expressing resource capabilities according to AARC-G027. Capabilities define the resources or child-resources (e.g. RCauth Online CA, GOCDB) a user is allowed to access.

v19.09.3 - 2019-09-12

Fixed

- Fix bug in IdPs buttons CSS style in IdP Discovery page (WAYF)

v19.09.2 - 2019-09-03

Added

- Add support for hiding enrolment attributes from the user registration form: By default, all the configured Enrolment Attributes are displayed in the enrolment form. Admins can control which attributes are displayed by configuring the visibility of the enrolment attributes.

v19.09.1 - 2019-09-01

Added

- Add support for additional login options:
    - Bitbucket
    - Github

v19.08.1 - 2019-08-21

Added

- Add support for storing the Authenticating Authority during user registration. The Authenticating Authority is displayed in the profile of the user under their linked organisational identities panel.

v19.07.2 - 2019-07-17

Added

- Add support for generating given name and surname attributes based on the full name information received from the identity provider

v19.07.1 - 2019-07-09

Added

- Add support for the OAuth 2.0 device authorization grant: This grant is designed for Internet-connected devices that lack a browser to perform a user-agent-based authorization (https://tools.ietf.org/html/rfc8628)

Changed

- Update style of Google login button displayed in IdP Discovery page (WAYF).

Fixed

- Add "refresh_token" to "grant_types_supported" which was missing from the well-known OpenID configuration

v19.06.1 - 2019-06-21

Added

- Add support for IdP hinting in the RCauth plugin to allow fetching the User's Subject DN from RCauth without manual IdP discovery. The administrator of the RCauth plugin can provide the IdP hinting url in the plugin configuration page.

v19.05.3 - 2019-05-20

Fixed

- Fixed permissions issue which prevented users from viewing information about their linked identities.

v19.05.2 - 2019-05-13

Fixed

- Fix bug where the user's email status remained unverified after successful verification of their email during registration

v19.05.1 - 2019-05-09

Added

- Add "hidden" functionality to Enrol page of the Group Management framework. The Administrator user can enable the functionality by changing the value of `Hide Enrolment Flow` field to true, in the config page of an Enrolment flow. By default the value is

false/empty and all the configured Enrolment Flows will be displayed in `People->Enroll` page

v19.04.1 - 2019-04-19

Added

- Add RCauth plugin to allow users to link the subject DN of their certificate issued by RCauth
- Add VOMS (de)provisioning plugin:
    - handles the (de)provisioning of users' participation in Collaborations or Groups in VOMS (Virtual Organization Membership Service) server
    - Interacts with VOMS server via the utilization of the user's Subject DN retrieved from MasterPortal
- Add search functionality to group membership management page. Users can be filtered/sorted:
    - by Given Name
    - by Family Name
    - by Email
    - by Identifier
    - Alphabetically
- Add search functionality to groups page. Groups can be filtered/sorted:
    - by Name
    - by Description
- Add search functionality to enrolments flow page. Enrolments can be filtered/sorted by Name

Changed

- Use common EGI theme across all user-facing interfaces of Check-in

Fixed

- Prevent users from submitting multiple registration requests
- Handle multiple attribute values for email and subject DN upon registration
- Pagination functionality added in order to handle any error(s) occurred while managing large group memberships

v19.01.1 - 2019-01-07

Fixed

- Fix JSON header in response from well-known OpenID configuration

2.2.3 2.2.3 Future plans

- Improve integration with EUDAT B2ACCESS [Q1 2020]
- Add support for retrieving Proxy certificates through SSH key information managed by the EGI Check-in COmanage Registry [Q1 2020]
- Scope-based active attribute value selection: This enhancement will allow OAuth2 clients to limit the values of specific claims based on the requested scopes [Q1 2020]
- Improve the identity linking user experience and interface [Q2 2020]

- Improve linked identities panel by including localised friendly name & logo of user's IdP
- Enable implicit identity linking

- Add support for (de-)provisioning and continuous update of user account information:
  - SCIM [Q4 2020]

2.3 eduTEAMS

2.3.1 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 to 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 (i.e.. 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.
TRL	9

2.3.2 Release notes

2019-11

Changed

- Upgrade to eduTEAMS v2
    - Upgrade to Debian 10 on all components
    - Upgraded SATOSA to v5.0.0-eduteams-0.0.1
    - Upgraded Consent Management Service to v3.0.0
    - Upgraded pysaml2 to v4.9.0
    - Upgraded micro services to v4.0.0

2019-10

Changed

- Upgraded eduTEAMS PyFF to v20191002.192717
- Upgraded Perun to v3.8.0

2019-09

Added

- Added support for multiple user identifiers in Perun
- Added support for Bitbucket as an authentication option

2019-08

Added

- Enabled the release of the new subject-id attribute
- Added extra scopes following the REFEDS whitepaper document on SAML to OIDC mapping: https://wiki.refeds.org/display/CON/Consultation%3A+SAML2+and+OIDC+Mappings

Changed

- Upgraded eduTEAMS SATOSA to v4.4.0-eduteams-0.0.3
- Upgraded eduTEAMS Consent Management Service to v1.1.1
- Upgraded pysaml2 to v4.8.0
- Upgraded eduTEAMS SATOSA micro services to v2.4.1
- Upgraded Perun to v3.7.0
- Enabled the release of eduPersonTargetedID with the value of CUID
- Improved the integration with HEXAA and COmanage

2019-07

Added

- Added new functionality to check whether IdPs release the expected attributes
- Added new functionality to whitelist SPs connected to eduTEAMS

Changed

- Upgraded eduTEAMS SATOSA micro services to v2.2.4
- Upgraded eduTEAMS Consent Management Service to v1.0.1
- Upgrade eduTEAMS webapp to v20190708.083021

2019-06

Changed

- Migrated to the new generator for user identifiers
- New version of the webapp

2019-04

Changed

- Javascript and CSS resources from Perun are now served from the Perun instance and not from a third-party CDN

2019-02

Added

- Added fail-over for Perun

2019-01

Added

- Added fail-over for COmanage and HEXAA

Changed

- Enabled Sirtfi and Coco on the eduTEAMS frontend (IdP)
- Enabled hide from discovery for the IdP interface of eduTEAMS Proxy

2.3.3 2.3.3 Future plans

- Upgrade to eduTEAMS v3
- Enable Active Attribute Selection feature
- Integration with the Step-up Authentication Pilot Service
- Support for AARC-G031 "Guidelines for evaluating the combined assurance of linked identities"
- Support for AARC-G021 "Exchange of specific assurance information between Infrastructures"
- New OpenID Connect Frontend
- Support for OIDC Federations

2.4 INDIGO IAM

2.4.1 Overview

Service/Tool name	INDIGO IAM
Service/Tool url	https://github.com/indigo-iam/iam
Service/Tool information page	https://www.indigo-datacloud.eu/identity-and-access-management
Description	The INDIGO IAM (Identity and Access Management) service provides user identity and policy information to services so that consistent authorization decisions can be enforced across distributed services.

Value proposition	• OpenID connect provider based on the MitreID OpenID connect library • SCIM user provisioning and management APIs • SAML authentication support • OpenID Connect authentication support • Flexible OAuth token exchange support
Customer of the service/tool	Research Communities
User of the service/tool	Users who need to translate credentials from different infrastructures and different authentication protocols.
User Documentation	https://indigo-iam.github.io/docs/v/current/user-guide
Technical Documentation	https://indigo-iam.github.io/docs/v/current/admin-guide
Product team	INFN
License	Apache License Version 2.0
Source code	https://github.com/indigo-iam/iam
Testing	Internal continuous integration test suite: https://sonarcloud.io/dashboard?id=indigo-iam_iam
TRL	9

2.4.2 Release notes

[1.5.0] - 2019.10.25

ADDED

- It is now possible to configure multiple external OpenID Connect providers.
- IAM now supports group managers. Group managers can approve group membership requests.
- It is now possible to define validation rules on external SAML and OpenID Connect authentications, e.g., to limit access to IAM based on entitlements.
- Real support for login hint on authorization requests: this feature allows a relying party to specify a preference on which external SAML IdP should be used for authentication.
- Improved scalability on user and group search APIs.

- IAM supports serving static local resources; this support can be used, for instance, to locally serve custom logo images.
- Actuator endpoints can now be secured more effectively, by having dedicated credentials for IAM service deployers.
- It is now possible to configure IAM to include the scope claim in issued access tokens.
- Support for custom local SAML metadata configuration.
- Improved SAML configuration flexibility.

FIXED

- Stronger validation logic on user-editable account information.
- EduPersonTargetedID SAML attribute is now correctly resolved.
- The token management API now supports sorting.
- Orphaned tokens are now cleaned up from the database.
- A bug that prevented the deployment of the IAM DB on MySQL 5.7 has been resolved.
- Support for the OAuth Device Code flow is now correctly advertised in the IAM OpenID Connect discovery document.
- The device code default expiration is correctly set for dynamically registered clients.
- The `updated_at` user info claim is now correctly encoded as an epoch second.
- IAM now defaults to transient NameID.

[1.6.0] - Unreleased

ADDED

- Improved token exchange flexibility
- Support for multiple token profiles (WLCG JWT profile, AARC G002 profile)
- Store and manage a URL pointing to the AUP document instead of the AUP text in the IAM dashboard

2.4.3 Future plans

- About the next IAM release v1.6.0 there are some dashboard and API fix/improvements already planned, for example:
    - IAM should allow customisation of the position of login page UI elements.
    - User may change registration name, email, etc when registering via SAML.
    - The registration approval page should show more information about user authentication.
    - The token management API should not expose token values to privileged users.
- Harmonization activities:
    - Alignment of user attributes following the REFEDS-R&S attribute bundle.
    - Alignment of resource capabilities information according to AARC-G027.
    - Alignment of affiliation information according to AARC-G025.
- The main development task is the transition to Keycloak as the main IAM authentication engine. Keycloak is a flexible and popular open source solution by Redhat for centralized authentication and authorization. Integrating Keycloak in IAM will provide enhanced capabilities and improved sustainability.

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 standalone 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.
TRL	9

2.5.2 Release notes

[v3.8.0] - 30. 9. 2019

- Old implementation of LDAPc component is now removed from sources. We use new implementation, which uses original module name perun-ldapc. Schema of LDAP must be updated according to state in: perun-utils/ldapc-scripts/schemas/perun-schema.ldif file. New LDAPc fills also Facility object and its attributes, displayName and eduPersonOrcid to User object.
- We are moving towards separation of attribute value checks in between syntax and semantics. There are new methods in API checkAttributeSyntax() and checkAttributeSemantics(). Original method checkAttributeValue() is still present, but is marked as deprecated and will be removed in next release 3.9.0).
- Virtual attributes no longer have value calculated in audit log. Any reader of audit log (e.g. LDAPc) must be able to read new AuditEvent objects and ask for value by itself.
- Support ExternalSources which provide multiple identifiers of user. When user logs into Perun, all provided identifiers are tried to match User in Perun (in use by eduteams proxy).
- Added new role PERUNOBSERVER, which can read everything, but can't modify anything. For now only in API, GUI support will be in next release.
- Overall speed improvement when synchronizing large groups and committing large transactions.

CORE

- Fixed attribute dependencies resolving when attribute is deleted.
- Fixed user categorization when we change ExtSource used for group member synchronization on group. As a result, we keep members which are matched from the old and new ExtSource. They are no longer unnecessarily removed and added.

- Fixed BBMRI registration module to support multiple collection directories.
- Added trigger logic when member is removed from group. It allows to move member to different groups. Kind like life-cycle workflow, but opposite direction is not allowed.
- Removed perun-rpc-lib modules.
- Removed module for min/maxGID attributes, we use GID ranges attribute.
- Added getData() methods which filter out expired group members.
- Improved performance on audit messages for big transactions. We no longer calculate the value of virtual attributes in messages and we discard duplicates of resolved messages (consequent changes) in one transaction. Fixed BBMRI registration module to support multiple collection directories.
- New type of ExtSource TCS, for importing certificates.

LDAPC

- Removed old implementation from sources (module perun-ldapc and perun-ldapc-initializer). We now use only new implementation with module perun-ldapc (renamed from perun-ldapc-ada).
- Fixed handling of Vo, Group, Resource objects.
- Do not delete entities on sync, when loading data from Perun fails on DB error.
- New object Facility contains now the same set of attributes as Resource, we will migrate all facility attributes to Facility object and they will be removed from Resource for future use of resource attributes.

GUI

- Added support for setting windows destination types.
- Fixed constant refresh issues on some pages (especially application pages).

CLI

- Fixed authz in CLI, password can contain "/".

API

- Added methods to work with a list of members, so you can add/remove group members with single callback.
- Fixed exceptions thrown when creating entities (vo/group/...). It's no longer just InternalError when we know, that one parameter contains a disallowed character.
- Facility manager can call getAssignedFacilities().
- Method checkAttributeValue() will be removed in next release, it is replaced by checkAttributeSyntax() and checkAttributeSemantics()

OTHER

- Apply timeout for KDC password manager. It prevents perun to be stuck when KDC has locked DB.
- Updated RPC documentation.
- Update to Spring 5.1.9.

[v3.7.0] - 22. 7. 2019

- This version contains DB changes and they must be applied when Perun is shut down!
- Because of changes in AuditMessage object this version requires equal version of all consumers - e.g LDAPc to be deployed at the same time.

CORE

- Reverted changes to BBMRI lifescience hostel modules.
- Ignore AlreadyMemberException in BBMRI modules.
- Split relation to perun attribute in registration form items into source and destination attribute. Form item value can be then pre-filled from different attribute than stored or doesn't have to be stored or pre-filled at all, based on your settings.
- Switching member to EXPIRED state will now trigger attribute validation (when former state is INVALID or DISABLED).
- Added "lastAccess" property to UserExtSource and display it in administrative GUI.
- Added suspended and suspendedTo params to Member and RichMember objects. They will hold a suspension state of Member in the future, while SUSPENDED member status will be removed from the life cycle. It is not used anywhere yet, except the member object. Regarding deserialization, "suspendedTo" is required (null or date in string format), while "suspended" is a boolean flag derived from the current date and its relation to "suspendedTo" property.
- Added methods to set or removed new suspended state for member.
- Enabled locking of groups members during add/remove group member operations. It will prevent any future inconsistencies in group memberships caused by complex group relation structures and synchronizations and manual changes. Rework of internal AuditMessage / AuditEvent handling. We now exclusively use JSON format of messages. It still contains original string data but wrapping object and API has changed and required proper version of all consumers (eg. LDAPc).
- Removed support for sending notifications to Jabber service.
- Support group synchronization in exact times (specified as list of HH:MM rounded to 5 minutes).
- Store also start time of last successful group synchronization.
- Fixed unnecessary session initiation for BA/Kerberos authz.
- Fixed format of audit message for planned service propagation.
- Fixed setting authz to members group for VO managers.
- Fixed bad sql when checking security manager role for user.
- Fixed user resolving for user:virt:loa on user deletion.
- Fixed attribute module for systemUnixGroupName which prevented value deletion even if group was not system unix group.
- Added requestor to message body, when errors are reported to the mail address instead of mail.

LDAPC

- Big improvements of LDAP initialization performance in new LDAPc.

- Fixed removal of non-existent entries from LDAP during sync.
- Allow oracle driver inclusion during build of new LDAPc.

GUI

- Delete VO members using single callback for list of members.
- Fixed message in GUI when user changes mail.
- Show new settings related to the group synchronization in pop-up window for group sync state.

API

- Big rework of AuditMessagesManager API.
- AuditMessage now contains AuditEvent instead of simple string message. It is still mainly used to read audit events/messages data.
- Added getAttributes() method for resource, group and member which will retrieve attributes for all related entities, including facility and resource.
- Added new methods to AuthzResolver getUser/GroupRoles().

CLI

- Added CLI for listing facilities by owner.
- Support SPONSOR role in setRole unsetRole tools.
- Added tools listOfExpiredGroupMembers and listOfNotExpiringGroupMembers which can list members and show their group expiration.

OTHER

- Removed unused default oidc settings for devel.
- Removed unused auditer-exporter module.
- Removed TextFile and SvgImage deserializers. Removed GraphViz library responsible for drawing attribute dependencies images. It will be returned as a string and UI app will draw the graphs. Removed all references for unused auditer_subscribers table.
- Updated Spring to 5.1.8.
- Updated RPC API docs for moveGroup() and some other methods.
- Removed all custom JSON, CSV parsing, we exclusively use jackson library (v2).

[v3.6.0] - 22. 6. 2019

CORE

- Added new configuration options for HikariCP in jdbc.properties.
- SMTP configuration was moved and joined from notifications module and registrar module into core (perun.properties).
- Added AuditEvent about user becoming perun admin.
- Check also large attributes previous value before performing update to prevent unnecessary checks and hooks when value doesn't really changed.

- Allow specifying mail notification templates for preferred mail change and password reset in entityless attributes (per namespace/language).
- Extended Group object definition in CLI.
- Fixed regex applied to elixirScopedAffiliations.
- Autocreate required namespaced attributes, supported namespaces can be specified in perun.properties.
- Added module for user:virt:eduPersonEntitlement which will gather eduPersonEntitlements from all users identities.
- Resolve user:virt:loa attribute changes when UserExtSource is updated so that LDAP is updated correctly.
- Removed duplicates in result of getGroupsMembersExcept*().

LDAPc

- Both old and new LDAP connectors now remove members from the group, if their group status in perun is not active. Behavior for vo status didn't change.
- Fixed handling DN of group names in new LDAPc.
- New LDAPc will now push only valid member on re-initialization.
- Added "loa" and "isCesnetEligible" attributes to the LDAP. LDAP schema must be updated before deploying this version!

GUI

- Do not load jQuery anonymously in GUI to prevent bug in Safari browser blocking it.
- Fix displaying wether group is authoritative for member synchronization.
- Inner tabs cross button (top-right corner), will perform same default action as do Close and Done buttons do. Eg. refresh underlaying tab after members were added to group.
- Fixed adding group member in GUI when user was already indirect member.

API

- Added method to getSponsoredRichMembers() with attributes.
- Extended getData() like methods which will automatically exclude expired members from the returned groups.
- Added API methods get(Rich)GroupsWhereUserIsActive(), which returns users groups filtered by facility or resource they are assigned to and also where member is in VALID state for both VO and Group.
- Added new method getRichGroupsAssignedToResourceWithAttributesByNames() with possibility to specify member and attrNames for member-group attributes.
- Added possibility to specify entity ID for methods like is[Entity]Admin().

OTHER

- Error reports from GUI can be directly send to mail address instead of RequestTracking system.
- Perun gathers also entitlement and assurance attributes from IDPs.

- Module for attribute user:virt:userOrganizations with mapping of VO names to user organizations (specified by member attribute).
- Fixed RPC docs for sendPasswordResetLink.
- Prevent possible duplicates in getAllowedUsers() when user was assigned through multiple resources.
- Changed login namespace for lifescience-hostel registrations to BBMRI namespace.
- Added CABINETADMIN role for publication management.

[v3.5.0] - 11. 3. 2019

CORE

- We now use HikariCP instead of ApacheDBCP for DB connection management.
- Fixed switching expired state for group expirations.
- Implemented logic for group membership expiration notifications.
- Added new perun-ldapc-ada module which will be used instead of current LDAPc in the future.
- Fixed wrong using of namespace in defaultUnixGID attribute module.
- Registrar now have configurable SMTP connection for sending notifications just like the core notification module.
- Support multi-lang links in password reset notification.
- Pass login-namespace in password reset notification links.
- Ported changes for user:virt:eduPersonScopedAffiliations, now it takes affiliations also from group:def:groupAffiliations.
- Removed support for user:virt:elixirBonaFideStatus, was replaced by new attribute user:def:elixirBonaFideStatus.
- Audit log messages are now stored and read as JSON and perun-engine component use instantiated classes to distinguish interesting messages. We will remove old DB table with custom serialized objects in future releases.
- Reading data from DB based on large list of IDs was reworked to use SQL array instead of constructing long SQL with ids. This give us time-consistent performance on each such select. This change requires DB schema to be updated to version 3.1.52
- Membership expiration calculation logic now uses Java 8 Date API.

GUI

- Use locally sourced jQuery in administrative GUI instead of their CDN.
- Added threshold for keepAlive checker in administrative GUI to prevent showing annoying pup-up on unreliable connections.
- You can now store "reason" why member in VO was suspended.
- Support to set new SELF_VO and SELF_PUBLIC rights on attributes.
- Password reset gui supports better theming and checks per login-namespace.

API

- Added new API method getMemberRichGroupsWithAttributesByNames().
- Support for paging in getAllRichGroupsWithAttributesByNames().

- Added utils method to API get Peruns current time (utils/getPerunSystemTimeInMillis).
- Allow force deletion of Facility.

OTHER

- Life Science hostel logic moved from login module to registrar module.
- Fix usage of MemberGroupAttributeRowMapper in getRequiredAttributes().
- Omit auditing messages about deleted attributes, if none was really deleted.
- We removed default logging from PerunException. Each exception must be now explicitly logged in the code. As fallback specific logger was created, so we can still get logs the old way. This will be removed in future versions.
- Methods to generate provisioning data are now in serializable transaction isolation to make sure generated data are consistent.
- Added CLI tools to switch Users between normal, service and sponsored state.

[v3.4.0] - 22. 1. 2019

CORE

- Merged code for attribute values caching, which should greatly improve performance. It's disabled by default in this version and will be subject to further testing on each instance.
- Attribute modules for determining group membership expiration from member_group, member_resource and user_facility context.
- Fixed vo membership expiration calculation.
- Fixed vo membership expiration notifications.
- Prefer native language when sending pwd-reset link from GUI.
- Allow password reset to random value for perun admins. PDF with password and generic text is returned. This is used by user-support. PDF template is configurable per namespace (can be any XHTML document).
- Added attribute modules for storing a reason why member has been suspended. All attribute modules can now listen to audit log messages (previously only virtual attributes could).
- Remove blocked destinations from the list of destinations where perun will push data to.
- Added new role - ResourceSelfService. Such user can assign or remove group from resource, if he's also group manager of the group.
- Added new sub ActionTypes for the SELF roles, so some attributes can be read/written if a user is related to the entity through his vo membership or it is supposed to be just public.
- Support for lifescience-hostel login namespace.
- Fixed group deletion when group was granting administrative role.
- Allow facility managers to read group attributes of assigned groups.
- Added modules for eduteams login namespaces (eduteams-acc-nickname, eduteams).

REGISTRAR

- Fixed use-cases for Elixir, when the user continues through multiple VOs forms.
- Bigger and colorful continue button to make sure the user doesn't miss it and doesn't close the browser.

GUI

- Manage values of entityless attributes from GUI (visible to perun admins only).
- Sort TaskResults by timestamp in reverse order (newer first).

OTHER

- Upgraded to Spring Boot Starter parent 2.1.2 / Spring 5.1.4.
- Perform CI tests on Ubuntu 16.04 and both JDKs (8, 11).
- CLI: Added tool to copyResource (with improved performance on server side).
- Cleanup parm names and order respecting attribute namespaces.
- Fixed tests on newer HSQL DB, since there was a change in compatibility mode regarding create index SQL command.

2.5.3 Future plans

Perun development is mostly driven by requirements coming from user communities. Therefore, the plans for its future development are rather brief, leaving enough space for reacting on newly emerging requirements.

Long term development plan contains the following:

- Performance optimization
- New graphical user interface
- New user profile interface
- Redesign workflow for account linking
- Improved integration with authentication proxies
- Pentesting
- Improved user documentation
- Automatization of operation process
- New component for user registration
- New roles and authorization module
- Improved process for the synchronization of users, attributes and group from external systems

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, among others, IGTF compatible (IOTA) X.509 certificates, including certificates obtained from an online CA (such as RCauthCA). Additionally, it supports plugin-based functionalities, where access to these functionalities is discriminated based on received attributes. Additional functionalities include deployment of SSH keys, obtaining SSH certificates (in conjunction with having an SSH CA), access to storage service (e.g. object storage), and others.
Value proposition	Allow to (transparently) create X.509 certificates for a user. This makes usage of grid infrastructures easier (user does not have to see the certificate). It also supports providing VOMS certificates to users and services. Furthermore, the service supports REST API, and therefore can provide these certificates via REST (which includes CLI access).
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
TRL	9

2.6.2 Release notes

[v1.7.0] - 2019-08-1

- Support for systemd unit files on debian

[older releases]

- Improve oidc libraries to support additional jwk headers
- remove insecure ciphers
- support for password (used to store and obtain secrets, such as OIDC client_secret)
- communicate with plugins using stdin, instead of environment variables

2.6.3 Future plans

Provide distributed architecture (with a distributed database) to easier deploy HA scenario.

2.7 MasterPortal

2.7.1 Overview

Service/Tool name	MasterPortal (reference service)
Service/Tool url	multiple instances accessible via REST API (no typical UI): https://aai.egi.eu/; https://masterportal-pilot.aai.egi.eu/ (EGI development instance); https://elevator.nikhef.nl/; 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/RCauth.eu_and_MasterPortal_documentation
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. It forms a 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 it provides the capability to upload SSH public keys and to retrieve proxy certificates using those.

Value proposition	Allowing the use of 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/RCauth.eu_and_MasterPortal_SSH_Key_Portal - end-users https://wiki.nikhef.nl/grid/RCauth.eu_and_MasterPortal_VOPortal_integration_guide - VOportal developers/operators
Technical Documentation	https://wiki.nikhef.nl/grid/RCauth.eu_and_MasterPortal_documentation
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)
TRL	9

2.7.2 Release notes

[v0.2.0] - 2019-08-29

All components:

- Fixed
    - Moving to 4.2 release of upstream dependencies OA4MP and security-lib, fixing many (upstream) bugs

MasterPortal component:

- Changed
    - If you are upgrading from a previous release, you will need to make several changes to the client and server config files.
    - Scope handling has changed, and it is now necessary to explicitly enable the set of supported scopes for each client separately.
- Added
    - When using the ssh key API, you can now restrict it to a specific scope
    - It is now possible to manage clients (i.e. MasterPortals) also using a JSON-based REST API (/clients) making use of special administrative client credentials.
    - Using the new /revoke endpoint, clients can now revoke their own refresh tokens.
    - it is now possible to configure a client to *only* receive limited proxies.

VO portal component:

- Changed
    - If you are upgrading from a previous release, you will need to make several changes to the config file.
- Added
    - In addition to plain proxies, it is now possible to directly obtain VOMS proxies via the VO portal.
    - By default, the portal now prints the user's username (sub claim). Additionally, you can also view the rest of the received claims (userinfo response).

SSH keys portal component:

- Changed
    - If you are upgrading from a previous release, you will need to make several changes to the config file.
- Added
    - By default, the portal now prints the user's name (*name* or *given name+family name*), username and IdP's display name. You can configure which claims are used for each of these

2.7.3 Future plans

Integration with the ssh-key upload capability of EGI's COmanage has been implemented in the EGI development instance and is also planned for the production instance of the EGI MasterPortal. A plan for creating a HA setup has been made and it is planned to test this setup in a development instance.

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 a token translation service (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/Master_Portal_Administrator_Guide Science GateWay operators/developers: https://wiki.nikhef.nl/grid/RCauth.eu_and_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 an Ansible virtual container environment (accessibility testing of the operational is performed with nagios from within the operating site)
TRL	8

2.8.2 Release notes

[v0.2.0] - 2019-08-29

- Fixed
  - Moving to 4.2 release of upstream dependencies OA4MP and security-lib, fixing many (upstream) bugs
- Changed
  - If you are upgrading from a previous release, you will need to make several changes to the client and server config files
  - Scope handling has changed, and it is now necessary to explicitly enable the set of supported scopes for each client separately.
  - In order to use mail notifications, it is now necessary to provide tomcat with the javax.mail.jar file.
- Added
  - It is now possible to manage clients (i.e. MasterPortals) also using a JSON-based REST API (/clients) making use of special administrative client credentials.
  - It is now possible to configure a client (i.e. a MasterPortal) to *only* receive limited proxies.

2.8.3 Future plans

Future plans for RCauth are split into three parts - setup of HA RCauth, Production RCauth, and anything else. Completed tasks are not listed, but larger tasks that are ongoing are listed.

2.8.3.1 High Availability RCauth (Task 5.1.8)

- Key cloning (ongoing)
    - Key exchange (ongoing)
    - Install keys in HSMs (GRNET and STFC)
- Database
    - Database synchronisation secure networking
    - Database deployment
    - Test synchronisation (ACID)
- Deployment
    - Code refactoring (as needed) to deploy at other sites (ongoing)
    - RCauth signing service deployment at STFC and GRNET and interfacing to HSMs (and other site-specific infrastructure, such as monitoring)
- Testing HA

2.8.3.2 Production RCauth (Task 5.1.7)

- Improve documentation for users and admins [5.1.7.1]
- User support
- Monitoring (as a cross-site service)
- Performance and metrics (as a cross-site service)
- Compliance audits
- Service business continuity and disaster recovery planning

2.8.3.3 Other

It is expected that some work may need to be done in WP13 to improve the user experience of the AAI stack, based on the results of the experience of using the integrated stack and user feedback.

3 Marketplace and Order Management tools

3.1 Marketplace

3.1.1 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/Marketplace (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.
TRL	9

3.1.2 Release notes

In this document we enclose only the most significant releases. The rest of them with details can be found in GitHub.

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

[1.1.0] - 2019-01-18

Added:

- support for backoffice (breadcrumbs, possibility of adding service offers, service portfolio manager role, statuses for services)
- JIRA mapping for new fields in Marketplace

Changed:

- unification of backoffice and admin layout
- adding many owners to the service

Fixed:

- typos in terms and conditions

[1.2.0] - 2019-01-29

Added:

- “Research area” in service form
- Implementation of features enabling voucher-based orders - Helix Nebula use case (JIRA integration, emails, styling, new custom fields)

Fixed:

- show error when research area is not selected

- show * near research area field
- RWD for offer selection
- remove shell command invocation in one of the test

[1.4.0] - 2019-02-26

Added:

- further support for vouchers (emails, voucher id on project item view)
- support for three types (normal, open access and catalogue) offers in backoffice
- validation for data type of attribute

Changed:

- names of buttons and headers
- emails for vouchers
- styles for project item details

[2.0.0] - 2019-08-06

Added:

- task for importing service data from eIC
- possibility to edit services and service offers by service owners
- project field is automatically prefilled if you add the service from the project view

Changed:

- country of customer and country of collaboration fields (with JIRA transition)
- new implementation of the Marketplace Projects as a lightweight approach to allow users to organise their orders, reflect a common purpose and gain support from EOSC experts in the scope of the created project

Removed:

- affiliation

Fixed:

- showing projects with empty countries of partnership list
- wrong redirection after logging in
- disabled possibility to add offers in drafts
- vulnerabilities alert

[2.2.0] - 2019-10-18

Added:

- User feedback based enhancements of service visibility and discoverability in the MP (filters autoreload, service preview in backoffice, multi checkbox filters search, project creation time default ask a question for non-signed in users, all filters expanded by default, filters title in active filters)

- "Publish as unverified" button to the Backoffice for services that were pulled from eIC but was not verified by onboarding team yet
- propagate project info update to JIRA

Changed:

- User Interface fixes and upgrades

Fixed:

- EOSC Portal component titles at the top bar
- hide scrollArrow in scroll event

3.1.3 Future plans

1. Development and implementation of a new service access and ordering models
2. MP Backoffice - further cooperation with onboarding team and service owners
3. MP Backoffice - further support for offers
4. Improvement the service interoperability levels - bundle concept introduction
5. Implementation of Helpdesk Interface on front page of the MP.

3.2 Service Portfolio Management Tool (AGORA)

3.2.1 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 allows the service management according to the 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.
TRL	8

3.2.2 Release notes

Agora Service Portfolio Management Tool

[Unreleased]

Added

- Add footer.

[0.9.16] - 2019-08-27

Added

- Expose components to anonymous users.
- Expose component connections to service versions to anonymous users.
- Basic setup of e2e testing using Cypress.
- Provide dummy user data for Dockerfile.

- Messages using Argo Messaging Service contain more information.
- Add new menu item "My Services" for serviceadmin users.
- Add icons to navigation menu items.
- Add profile page.

Removed

- Remove unused /api/v2/my-services endpoint.
- Hide "Service Versions" from sidebar menu for serviceadmin users.

[0.9.15] - 2019-06-19

Fixed

- Correct redirect url when connecting a component to a service version and a version to a service.

Removed

- Remove unused code, mainly referring to api/v1.

[0.9.14] - 2019-06-12

Changed

- Do not expose sensitive data (service owner, security and support contact info) in public api.

Fixed

- Fix bug preventing service providers from saving.

[0.9.13] - 2019-06-03

Added

- Provide UI for Agora by merging [agora-admin](https://github.com/grnet/agora-sp-admin) repository.

[0.9.12]- 2019-05-23

Added

- Add Organisation model exposed in /providers endpoint.
- Add Access Policy model.
- Add Federation Member model.
- Services can belong to organisations.
- Service admins can be assigned to organisations by superadmins.
- Add related/required services to Service model.

Changed

- Upgrade apimas to 0.4a4.
- Extract ServiceDetails permission fields dynamically.

- Rename Service Area -> Service Category.
- A Service can belong to many service categories.
- Add/remove fields to models according to new guidelines.
- Models altered are: Service, ServiceDetails, ServiceStatus, User.

Fixed

- Various pep8 fixes.

[0.9.11] - 2019-03-05

Added

- Service admins can create components related resources.
- Service admins can create/edit CIDL for services they own.
- Service admins can create/edit Service Versions for services they own.

Fixed

- Trim Service name before saving.

Security

- Update Django version to fix vulnerability issues.

[0.9.10] - 2019-02-12

Fixed

- Enable partial update actions for admins/service admins.

[0.9.9] - 2019-02-07

Changed

- Upgrade apimas to 0.4a3.
- Use specular instead of docular.
- Update testing code to match latest pytest deprecation notes.
- Expose Service external/internal contact information as struct.

Fixed

- Use default values in spec for not nullable fields in model.

Security

- Update Django version to fix vulnerability issues.

[0.9.8] - 2019-01-03

Added

- Expose more fields to service-types endpoint.

3.2.3 Future plans

Support, maintain and extend the Agora Service Portfolio Management Tool in order to

- add support for SDT V1.3 and 2.0 & SDT for federating core service
- add support for the onboarding procedure,
- Integration of SPMT with EOSC Portal and EOSC Configuration Management System.
- add support to provide topology for Argo Monitoring

4 Integrated Business and Operations Support Systems

4.1 Operations Portal

4.1.1 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	Home · Wiki · OpsPortal / sf3
Technical Documentation	Home · Wiki · OpsPortal / sf3
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
TRL	9

4.1.2 Release notes

v5.1 - 02/10/19

ROD dashboard: Improvements

- The template to open ticket again site is now completely visible - not only the part related to alarms.
- Fix problem with carbon copy emails sent with tickets / notepads

Service Order Management Back office - v1.1

- Add a view of all service orders (no authorization based on service) with additional filters
- Make some fields only readable in the summary of Jira issues (ask list to shifters)
- Adapt the list to the new structure of Jira issues (master / slave - epic)
- Adapt the workflow and the details on the type of ticket (epic or service order)
- Add the possibility to edit / remove providers and to add free provider
- Generate pages for service providers using tokens and send email with the url to inform them

VO ID cards

- correction of bugs for the declaration of resources
- correction of bugs for the registration of Vo contacts

v5.2 - 12/11/19

Vo Id cards

- Changes into the resources section (added in v5.1) are now reflected into the read only view (permalink)

Service Order Management Back office - v1.2

- Remove remaining mandatory fields
- Separate the form into 2 forms: one for epic issue, the other for service order issue
- Make the author of comments more visible (colour code)
- Correct bug with the access to some states of the issue
- Show details about orphan project
- Publish the Service Order to DPMT via AMS

4.1.3 Future plans

- Move documentation to Gitlab and update it
- Move from EGI Checkin to EOSC AAI
- Service Order Management Back office - v1.3
    - Implements a complete workflow for the SLA
    - Evaluate the possibility to provide usage reports (accounting, QA monitoring)

4.2 GOCDB

4.2.1 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.

TRL	9

4.2.2 Release notes

5.7.4 - 2019-08-19

Patches, Bug Fixes and Documentation Changes

- Replace icons used on GOCDB pages with new icons of known source and add a 'delete' icon.
- Allow "org.squid-cache.Squid" ServiceType to be production and not monitored.
- Fix GOCDB_monitor checks on SL7
- Add LICENSE file to GitHub repository

5.7.3 - 2019-04-29

Patches, Bug Fixes and Documentation Changes

- Replacement of broken Google Map with open source Leaflet map
- Add an Acceptable Use policy and a Privacy policy
- Enable ShibAuthToken authentication by default
- Bug fix when calculating downtime timezone offsets
- CSS and Documentation improvements.
- Spelling/Punctuation/Grammar and typo fixes
- Removal of unused files

4.2.3 Future plans

- Development of an EOSC-hub specific view on the data in GOCDB.
- Change in the underlying infrastructure of GOCDB to improve reliability.
- Fetching new service types from an EOSC-hub Service Portfolio Management Tool

4.3 Data Project Management Tool

4.3.1 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	not applicable
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.
TRL	8

4.3.2 Release notes

Added:

- Dedicated types for describing configurations of multiple specific endpoints for services such as iRODS or Handle that support multitenancy
- Overview pages for the newly introduced types mentioned above
- Various schema enhancements in response to concrete requests (e.g., adding a “VAT” property to the customer and provider types)
- Introduced service options to stay in line with the EOSC Service Catalogue
- Support for scoping of projects
- Introduced new icons for most custom types

Changed:

- Enhanced StAR view of accounting data to include metadata on related projects and customers
- Enhanced ‘get_service’ and related views in the GOCDB compatibility layer to include contact information on endpoints. This was in response to a request from the monitoring service.
- Adjusted the ‘service offer’ and ‘service request’ types to support specification of service options
- Various types now infer a scope from the project(s) they are related to and display it.

The full change log/commit history is available from

https://github.com/EUDAT-DPMT/pcp.contenttypes/commits/master

4.3.3 Future plans

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

4.4 Data Management Planning Tool

Here we only report on the EasyDMP tool that is part of EUDAT and the EESTORE that is developed within EOSC-Hub and is part of the OpenDMP tool that is a data management planning tool developed in collaboration with openAIRE.

4.4.1 Overview

Service/Tool name	EasyDMP
Service/Tool url	https://easydmp.eudat.eu

Service/Tool information page	https://www.sigma2.no/data-planning
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 (i.e. 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.
TRL	7

4.4.2 Release notes

A rolling release approach is followed where incremental releases are frequently deployed in production (the full list of releases can be seen in the git packages described in the table). Since the last version of this document the following functionality changes have been made:

EasyDMP

0.21.0 18-09-19

Added

- Change to how BooleanQuestions work and are stored based on the performance when filling in questionnaires.

0.20.0 12-09-19

Added

- Completed migration to new version of Django

0.18.0 20-03-19

Added

- Support for a new question-type: shortfreetext

0.17.0 08-03-19

Added

- Access cached section graphs from API and administration interfaces.

0.16.0 07-03-19

Added

- Support for optional questions.

0.15.0 01-03-19

Added

- New version of the Science Europe template (based on the open science guidelines https://www.scienceeurope.org/our-resources/guidance-document-presenting-a-framework-for-discipline-specific-research-data-management/)

0.14.0 14-01-19

Added

- Simple template design tools and linear templates

0.13.0 19-11-18

Added

- Multiple questions on a single page

EEstore

v2.0.0-alpha.1 08-11-19

Added

- New database layout for the second production version

1.0.0 17-07-19

Added

- Frozen production version receiving only bug fixes

0.14.0 27-06-19

Added

- Bug fixes, and rollback to Django 1.11

0.12.0 07-06-19

Added

- Auth-support and start of API for controlling plugins

0.10.0 10-05-19

Added

- Upgrades of the eestore third-party repositories and removal of the config endpoints.

4.4.3 Future plans

- To align the schema of EasyDMP with that of the Research Data Alliance (https://github.com/RDA-DMP-Common/RDA-DMP-Common-Standard/tree/v1.0#dataset_table) common DMP standard and to demonstrate the interoperability between EasyDMP and openDMP by exporting a plan from one tool and importing into the other.
- Support local deployments of the eestore and extend the resources harvested (to include the SPMT/DPMT).
- To onboard the OpenDMP tool into the EOSC portfolio of services.

4.5 Service Versions Monitoring Tool

4.5.1 Overview

Service/Tool name	SVMON
Service/Tool url	https://svmon.eudat.eu

Service/Tool information page	(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://wiki.eosc-hub.eu/pages/viewpage.action?pageId=61374702 (in progress)
Technical Documentation	https://gitlab.eudat.eu/jie.yuan/svmon-app/ (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 A testing instance https://svmon-dev-test.scc.kit.edu
TRL	8

4.5.2 Release notes

2.2.1 - 2019-10-28

Added

- Implementation of the token-based authentication for the svmon clients
- Updates of the clients at sites with two options to use svmon client: with authentication (standalone), integrated with pakiti - without authentication

2.1.0 - 2019-06-26

Fixed

- Suitable representation of shared "Sites" from both DPMT and GOCDB
- New HTTP API to get site information

2.0.1 - 2019-05-31

Changed

- Table paging numbers
- Add username

2.0.0 - 2019-05-06

Changed

- new version of Angular

1.0.4 - 2019-04-10

Changed

- Java keystore with E-Science CA

Added

- Data Privacy Statement
- 'EOSC-site' filter
- Back button, paging, searching in the front
- Direct http post from SVMON client

Fixed

- DPMT site report parser

4.5.3 Future plans

We will distribute SVMON client to all EUDAT service hosts. For the standalone version, we will add user token authentication to POST reports. We will continuously improve the web interface according to the community requests. And also, we will implement further harmonization of and filtration of data sources according to scope tag.

5 Monitoring, Accounting, Messaging and Security Tools

5.1 Accounting Repository

5.1.1 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.
TRL	9

5.1.2 Release notes

APEL

1.7.1 - 2018-11-29

Added

- Support for SLURM parser to use TotalCPU rather than CPUTimeRAW for CPU duration and updated suggested sacct script to match.

Changed

- Minor improvements to build process and setup.py script.

1.8.0 - 2019-01-07

Added

- Warning in client log if no records are unloaded during a run.
- Optional 'cputmult' factor to HTCondor parser to support its use as a parser for HTCondorCE setups.
- PID/process check to central summariser to prevent overlapping runs.

1.8.1 - 2019-07-03

Added

- Option to update client benchmarks/spec levels using a local configuration option rather than the BDII.

1.8.2 - 2019-09-03

Changed

- How cloud records are loaded so that the last received record for a VM in a month is kept (rather than the one with the latest timestamp). This simplifies things when sites republish cloud VM accounting.

SSM

2.4.0 - 2019-08-01

Added

- Support for sending and receiving messages using the ARGO Messaging Service (AMS).
- Option to send messages from a directory without needing to conform to the file naming convention that the dirq module requires.

Fixed

- SSM hanging if certificate is not authorised with the broker. Now it will try other brokers if available and then correctly shut down.
- An OpenSSL 1.1 syntax error by including missing value to argument that checks certificate expiry date.

2.4.1 - 2019-09-04

Changed

- Logging to remove excessive messages from a 3rd-party module used when sending via AMS.

Fixed

- Handling of OpenSSL errors so that messages that have been tampered with are now rejected.

5.1.3 Future plans

- Improvements to AMS integration, including making certificates optional.
- New interface and API for publishing and synchronisation tests.
- Enhancements to storage accounting.
- Fixes to SLURM parser.

5.2 Accounting Portal

5.2.1 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
TRL	9

5.2.2 Release notes

Added (Release 25)

- Support for Jupyter Notebook sites.
- Top CSV download button to Tier2 report.
- Project and customer views for Storage EUDAT.
- UserDN accounting to EUDAT views.

Changed

- Improved UserDN accounting treatment of Cloud metrics.
- Improved userDN cloud metric selection.
- Index optimization.
- Query optimization.
- Improvements to credential handling.

- Improve Project handling EUDAT.
- Improved unit handling code.

Removed

- EGI references in EUDAT pages.

Fixed

- Changed left join on tier2 report to avoid problems with DESY sites.

5.2.3 Future plans

- Improve EUDAT views
- Research the convenience and best way of integrating the eosc-accounting and accounting instances.
- Move Storage accounting to production after APEL changes
- Improve WLCG views
- Transition to AMS from SSM

5.3 Monitoring

5.3.1 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 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 [R3] is a command-line collection runner for Postman [R4]. It allows you to effortlessly run and test a Postman Collections [R5] 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.
TRL	9

5.3.2 Release notes

ams-consumer

Version 1.1.0

Fixes

- Fix dash typo in consumer systemd service file

Features

- ARGO-1262 Extend consumer schema with actual_data field

argo-alert

Version 0.2.0

Features:

- ARGO-2027 Split gocdb contain email string into individual items
- ARGO-1710 publish group item status info
- ARGO-1715 Consolidate alerts for endpoints that belong to multiple endpoint groups
- ARGO-1640 Update alert publisher to forward new event information

Fixes:

- ARGO-1793 Fix ui_urls in alert mails to point correctly to the new web_ui

argo-ams-library

Version 0.4.3

Fixes

- ARGO-1990 Fix runtime dependencies
- Make all print statements Py 3 compatible
- Obsolete old name of package for Python 2 deployment
- Refined spec for Py2 and Py3 building on CentOS6 and CentOS7

Features

- ARGO-1862 Make argo-ams-library Python 3 ready
- ARGO-1841 Update the ams library to include the new timeToOffset functionality
- Update to supported Python versions in Travis file

Releases

Version 0.4.3 https://github.com/ARGOeu/argo-ams-library/releases/tag/V0.4.3-1

Argo-egi-connectors

Version 1.7.3

Fixes

- ARGO-2017 - Token per tenants' config option
- ARGO-2013 - Metric profiles WEB-API connector
- ARGO-1549 - New helper tool that can replay avro data on AMS with customizable datestamp
- ARGO-1575 - Switch poem-connector to use new token protected POEM API

Version 1.7.2

Features

- Use requests library in connectors

Version 1.7.1-1

Features:

- ARGO-1428 ServiceGroup topology filtering
- ARGO-1370 Optimize connectors queries to POEM

Fixes

- ARGO-1269 Refactor poem-connector
- ARGO-1236 Datestamp of AMS msg does not match corresponding avro filename

Argo-nagios-ams-publisher

Version: 0.3.5

Fixes:

- include site name in metric result
- refactor body fields extraction from local result

Version 0.3.4

Feature

- Verbose log messages

Version - 0.3.3

Features

- ARGO-1624 Catch all exceptions and warnings from AMS

Version 0.3.2-1

Fixes:

- ARGO-1429 Improved msg counter stats for probe testing purposes
- ARGO-1408 Ensure correct permissions on pidfile directory

- ARGO-1348 Descriptive error in case delivery cache tool is called with queue path not specified in configuration files

Argo-ncg

Version 0.4.7

Features

- ARGO-1749 OCSP Nagios call should pass site name in metric result

Version 0.4.6

Fixes

- ARGO-1728 Change default SRM port
- ARGO-1729 NCG breaks on empty extension value
- ARGO-1690 Remove old JSON metric configuration from argo-ncg
- ARGO-1689 Remove POEM FQAN support from argo-ncg
- ARGO-1577 Refactor monitoring engine to use token protected POEM API

Argo-streaming

Version 1.3 - 2019-11-07

Features:

- ARGO-1963 Autoconfigure archiver subs and users
- ARGO-1932 Add dry-run mode to submission scripts
- ARGO-1980 Clean-up streaming status script submission
- ARGO-1931 Use proxy options in scripts for ams and web-api
- ARGO-1784 Streaming job: Remove decommissioned endpoints
- ARGO-1823 Alerts add synopsis list of metrics included in endpoint
- ARGO-1708 Extend event schema to include group item statuses ARGO-1709 Extend status streaming job to gather status info for all group items ARGO-1770 Remove failover for MetricData old schema

Fixes:

- ARGO-1974 Fix top level aggregations in streaming event generation
- ARGO-1786 Fix: mongo clean old endpoint_ar data
- ARGO-1785 Fix excluded monitoring data for previous day

Version 1.2 - 2019-03-22

Features:

- ARGO-1480 Argo engine automation: ensure mongodb indexes
- ARGO-1567 Remove restart strategy from batch jobs
- ARGO-1581 In status streaming job use optimistically OK as init status
- ARGO-1636 Extend status event schema
- ARGO-1675 Forward metric, endpoint and service values on all event levels
- ARGO-1679 Add batch endpoint a/r computation

Fixes:

- ARGO-1626 Status batch service aggregation OR/AND fix

- ARGO-164 Fix cron autoconfiguration daily/hourly mis-match
- ARGO-1652 Fix metric data schema migration in status streaming job
- ARGO-1740 Recomputation hdfs path fix

Argo-web-api

v1.8.1 - 2019-11-15

Fixed

- ARGO-2059 Fix latest strict result order by time instead of group name
- ARGO-2057 Fix latest results strict mode to honor limit & filter parameters
- ARGO-2058 Set strict=false by default in latest results call

v1.8.0 - 2019-11-04

Added

- ARGO-2038 Add version information to binary
- ARGO-2005 add extra information to tenants
- ARGO-2004 add extra information to reports
- ARGO-2003 Add a tenant list for web ui admin users
- ARGO-1997 Change recomputation status through web-api
- ARGO-1996 create recomputation: allow setting up recomputation requester name/email
- ARGO-1964 Return all daily metric data for specific host and date
- ARGO-1747 API Call - Get user by ID
- ARGO-1744 Add UUID for tenant's users

Changed

- ARGO-1727 Update the latest api call to be able to only return the latest entry
- ARGO-1983 Add filter param to return metric result list
- ARGO-1958 Fix add end of day point in multiple status timelines

Version 1.7.9-1 - 2019-03-22

Added

- ARGO-1438 Implement tenant general status
- ARGO-1680 serve endpoint a/r results

Changed

- ARGO-1455 - Migrate to golang/dep tool

poem

Version 2.3.0-1

Added

- ARGO-1573 Back reference fields on metrics and probes pages
- ARGO-1573 Back reference fields on metrics and probes pages
- ARGO-1693 Hover dropdown info about selected probe on metric page
- ARGO-1695 Support for deletion of Aggregation profile
- ARGO-1696 Style and arrange Aggregations page

- ARGO-1698 Aggregation profile permissions based on Aggregation group
- ARGO-1700 Introduce config option for specifying WEB-API endpoint
- ARGO-548 Introduce Aggregation profiles CRUD on WEB API
- ARGO-771 POEM multi tenancy support

Fixed

- ARGO-1719 Fix breadcrumbs for API key templates
- ARGO-1720 Fix Probe change form "Update metric" button
- ARGO-1724 Fix breadcrumb for Delete group pages
- ARGO-1688 Migrations are not registered as applied

Changed

- ARGO-1653 Refine log entries view
- ARGO-1681 Refactor service type sync to use Django ORM
- ARGO-1694 Refine comments in log entry details page

Version 2.2.0

Features

- ARGO-1580 Minimal container for tests
- ARGO-1572 Public profiles, probes and metric pages
- ARGO-1524 Introduce services and probes view
- ARGO-1501 Tests for API methods
- ARGO-1449 Add ability to browse all recent actions
- ARGO-1442 Token and session authenticated REST API
- ARGO-1442 Tests for authenticated REST API
- ARGO-1371 Make use of full-blown DBMS

Fixes

- ARGO-1628 Refine log entries view
- ARGO-1612 Fix tests by creating all needed tables in in-memory-DB
- ARGO-1568 History comments not rendered properly

Version 2.0

Added

- ARGO-1497 Publicly available Probes pages
- ARGO-1448 Active/Passive metric designation in metric configuration UI page
- ARGO-1309 Static Metric Config attribute with predefined keys
- ARGO-1370 Optimize connectors queries to POEM
- ARGO-1327 Update probe data without creating new version

Changed

- ARGO-1500 Reformat None/NULL field values fetched from DB to empty string in API views
- ARGO-1499 Do not allow probe name changes to existing probe
- ARGO-1485 Sorted autocompletion Metric entries
- ARGO-1482 Allow empty values for keys in metric configuration

- ARGO-1372 Use Apache and mod-wsgi from Software Collections
- ARGO-565 Move to Django 2.0 version

Fixed

- ARGO-1462 Plaintext LogEntry comments
- ARGO-950 Metric history browse always show most recent changes

Version 1.2.0-3

Features

- Configurable AAI login button
- Basic HTTP auth for service type syncing

5.3.3 Future plans

Continue to support, maintain and extend the Argo Monitoring service in order to add support for

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

5.4 Argo Messaging Service

5.4.1 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 [R3] is a command-line collection runner for Postman [R4]. It allows you to effortlessly run and test a Postman Collections [R5] 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.

TRL	8

5.4.2 Release notes

argo-messaging
The core messaging service.

v1.05.1 - 2019-09-05

New features/Enchantments

- ARGO-492 Add configuration parameter in the push configuration for max_messages per push action
- ARGO-1921 New API Call - Average daily messages
- ARGO-1880 List user members of a project
- ARGO-1670 Perform the RPC Subscription Status on api call Get subscription
- ARGO-1870 Add AMS metric: consumption rate on subscription
- ARGO-1834 Add AMS metric: publishing rate on topic
- ARGO-1828 API Call - Get offset from timestamp
- ARGO-629 When a topic is deleted in the api, ensure topic is also deleted in broker
- ARGO-1820 Update the messaging service to use the latest sarama version compatible with kafka 2

Fixes

- ARGO-1854 Change the way we utilise the sarama.ClusterAdmin in order to avoid EOF/broken tcp pipe errors

Removed

- ARGO-1892 Remove update subscription status functionality from the ams push server

v1.04.1 - 2019-07-03

New features/Enchantments

- Consumer script
- ARGO-1801 Update response Verify push endpoint call
- ARGO-1692 Upgrade authorisation per resource handling
- ARGO-1782 Adjust push worker workflow depending on the verification of the push endpoint of each subscription
- ARGO-1792 API Call - Verify Push Endpoint
- ARGO-1787 Add verification_hash and verified fields for push enabled subscriptions
- ARGO-1683 Block push worker user from pulling when push enabled is false
- ARGO-1723 Republishing of specific messages
- ARGO-1649 API Call that returns a user's profile based on the provided auth token

- ARGO-1721 [GRPC status check] - Update ams push server client to use the new status rpc call
- ARGO-1684 update status call to handle push enabled false
- ARGO-1669 Allow only push worker user to pull from push enabled subscription
- ARGO-1632 Add ACL-based access in subscriptions:list
- ARGO-1631 Add ACL-based access to topics:list
- ARGO-1657 Add/remove push worker from sub's acl and link him with sub's project
- ARGO-1661 Ams handling of push worker initialisation
- ARGO-1656 Internal function - append project to user's projects
- ARGO-1639 API Call - List topic's subscriptions
- ARGO-1651 Internal function - remove user(s) from topic/sub ACL
- ARGO-1650 Internal function - append user(s) to topic/sub ACL
- ARGO-1630 Push worker role
- ARGO-1604 Add health check call for grpc backends
- ARGO-1600 Add push server interaction on modify push config api call
- ARGO-1606 Update push status field api call
- ARGO-1602 Ams push server single connection
- ARGO-1553 Grpc client to interface with the push server
- ARGO-1471 Create a streaming producer
- ARGO-1469 Create a bulk producer
- ARGO-486 Add pagination support for project subscriptions
- ARGO-487 Add pagination support for project topics
- ARGO-1436 Mongo _id field exposure for pagination affects user creation
- ARGO-1432 Add pagination support for users
- ARGO-1431 Add daily msg count for projects:metrics
- ARGO-1427 Add daily msg count for topics:metrics
- ARGO-1401 Number of messages send via the Argo Messaging Service (per day)
- ARGO-421 Modify sub's ack deadline
- ARGO-1375 Script to export AMS kafka data
- ARGO-1827 Update connectivity logging format
- ARGO-1925 API support predefined policies in push mode subscription
- AO-492 Make syslog logging configurable for AMS
- ARGO-1825 Update the request logging format
- ARGO-1840 Update the error response for topic:publish and subscription:pull whenever a kafka error is encountered
- ARGO-1454 Migrate argo-messaging to golang/dep tool
- ARGO-1376 Extend ams-migrate script to support import
- ARGO-1554 Add a status field at the subscription struct that will contain information regarding its activation on the ams push server
- ARGO-1550 Disable push functionality in ams
- ARGO-1252 Update config to handle push server information

Fixes

- ARGO-1803 Update service file to include service restart on failure
- ARGO-1627 Check if the respective topic exists when pulling messages
- ARGO-1592 ACL for topic/sub should not contain empty names
- ARGO-1446 Improve the receiver endpoint to be more robust
- ARGO-1399 Topic:metrics && Subscription:metrics check if topic/sub exIsts
- ARGO-1410 Fix nil context bug
- ARGO-1373 argo-messaging add failsafe check to not allow admin empty tokens

Available Releases

- Version 1.0.5-1 - 5 September 2019: https://github.com/ARGOeu/argo-messaging/releases/tag/v1.0.5-1
- Version: 1.0.4-1 - 3 July 2019: https://github.com/ARGOeu/argo-messaging/releases/tag/v1.0.4-1

argo-ams-library

A simple library to interact with the ARGO Messaging Service.

Version 0.4.3

Fixes

- ARGO-1990 Fix runtime dependencies

Features

- ARGO-1862 Make argo-ams-library Python 3 ready
- ARGO-1841 Update the ams library to include the new timeToOffset functionality

Available Releases

Version: .0.4.3-1 - 8 November 2019: https://github.com/ARGOeu/argo-ams-library/releases/tag/V0.4.3-1

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.

Version: 0.1.3

New features/Enchantments

- ARGO-1773 Update authn scripts to filter service endpoints before creating the respective user
- ARGO-1615 update authn scripts to get site-mail from gocdb
- ARGO-1738 Add support for interacting with the argo-web-api
- ARGO-1737 Add support for headers auth method

- ARGO-1740 Change binding structure to be more generic

Available Releases

- Version 0.1.3 - 13 June 2019 - https://github.com/ARGOeu/argo-api-authn/releases/tag/v.0.1.3-1

5.4.3 Future plans

- Support, maintain, extend the AMS Service
- Support, maintain, extend the AuthN Service
- Support FedCloud Information System - AppDB: We maintain and adapt authn scripts to simplify the authentication of site/service providers to authn we support the smooth operation of the cloud information system with HAwe offer consultancy on how they can use the AMS more efficiently
- Support Accounting: Accounting is testing the service in order to use it. Some of the issues the Accounting team is facing is the size of the message they create and the metadata description to use. We are working together to solve and create the most suitable solution.

5.5 Security Tools

5.5.1 Pakiti

5.5.1.1 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.
TRL	9

5.5.1.2 Release notes

Pakiti-server v3.1.1 [2019-12-19]

Improved CLI

- Add --config option to some commands
- Enable importCvesTags to complain if an imported CVE doesn't exist locally.

GUI changes

- Add a vulnerability summary to the GUI
- List the source VDS, where the CVE is defined.
- List the number of current CVE occurences in the VDS list
- Remove year from the footers

Adaptation to export feed

- Changed the header of hosts report

New features and code improvement

- Move processing of vulnerability definitions to subsources
- Adding new functions to DAO and Managers
- Add calls to handle CVE's detected or maintained
- Add paging to CveDao's getNames()
- Make it possible to define multiple source definitions for Debian

Bug fixes and minor improvements

- Avoid using uninitialized array offsets
- Typo fixed
- Use only properly initialized variables
- Make sure that packages aren't marked by staled vulnerabilities.
- Don't store CVE definitions that don't list any CVE
- Make sure that Vulnerabilities don't contain stale records
- Enable parsing Debian LTS records
- Set the same access policy to CVE as to other modules
- Fix year in LICENSE
- Fix wording of a message

Pakiti-client v3.0.3 [2019-12-19]

Minor changes and adaptations

- Don't exit on unknown configuration options
- allow the proxy to override the host group in the report
- Change detecting OS from issue.net to os-release file

5.5.1.3 Future plans

- Addressing the needs of users based on evaluation of the pilot operation of Pakiti3
- Support and maintenance

5.5.2 Secant

5.5.2.1 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.
TRL	6

5.5.2.2 Release notes

2019-12-19

Support for OpenStack

- Migration of API
- Update queries for Openstack and parsing of output

Minor changes

- Fix cloud init check and creating internal error message.

5.5.2.3 Future plans

- Support and maintenance
- Finish integration with AppDB
- Finish support of OpenStack

6 Helpdesk Services and Tools

6.1 GGUS

6.1.1 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

TRL	9

6.1.2 Release notes

2019-11-27

* Decommissioned xGUS instances for NGI_DE, NGI_IT, NGI_SI, NGI_AEGIS, NGI_CH and FRANCE_GRILLES.

2019-11-27

* Install security patches

2019-09-18

* Install security patches

* Fixed bug: tickets automatically re-opened by system

* Upgrade ARServer to version 9.1.7

2019-07-31

* Install security patches

* Enable report "violated response time"

2019-05-22

* Install security patches

* Improve export of CSV/XML search results

* Use registered email instead of Cert DN email during ticket submit

2019-03-27

* Install security patches

* Grant GGUS support privileges for members of ggus-supporters in EGI AAI

* Implement dedicated issue types for ATLAS team tickets

* Implement email validation and sanitation

2019-01-30

* Install security patches

* Improve mailparser for recognizing external ticket IDs

* Modify VOMS synchronization

6.1.3 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 [R6], [R7].

6.2 EUDAT-RT

6.2.1 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 (page is protected)
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. The 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 (page is protected)
Technical Documentation	https://confluence.csc.fi/pages/viewpage.action?pageId=50874303 (page is protected)
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)
TRL	9

6.2.2 Release notes

The service has been in full production during this year, the only maintenance activities performed has been related to the infrastructure running the service. They were done on 5th and 6th August 2019 and implied the full stop and restart of the service.

During the last year no major improvements have been done, only minor changes about configuration of the queues and users, but none of them has implied any upgrade in the tool

6.2.3 Future plans

EUDAT-RT service is fully operational. The implementation of changes is done in the development version of the service and moved to production following the change management procedure of EUDAT-CDI.

No updates have been planned for the next year.

6.3 xGUS

6.3.1 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 (page is protected)
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	https://test.ggus.eu/EOSC-hub
TRL	9

6.3.2 Release notes

2019-12-04

* Move system from EGI AAI to EOSC Portal AAI

2019-11-27

* Install security patches

2019-09-18

* Install security patches

* Upgrade ARServer to version 9.1.7

2019-07-31

* Install security patches

2019-05-22

* Install security patches

* Implement the integration between EUDAT RT and EOSC-hub helpdesk (xGUS).

* Use registered email instead of Cert DN email during ticket submit

2019-03-27

* Install security patches

2019-01-30

* Install security patches

6.3.3 6.3.3 Future plans

Replace integration with EGI AAI by integration with EOSC Portal AAI

7 Application store, Software Repositories and other Collaboration Tools

7.1 Applications Database

7.1.1 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 [R8] 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 [R9].
TRL	9

7.1.2 Release notes

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

7.1.2.1 AppDB portal

[6.2.2] - 2019-07-19

Changed

- Forbid virtual appliance working versions to be verified if the VM image location URL use a self-signed certificate

Fixed

- Display proper IDs for OCCI and OpenStack endpoints

[6.2.1] - 2019-06-20

Added

- Added "authn" attribute to virtualization:provider and site:service XML elements in RESTful API

Fixed

- Fixed regression bug in scientific classification API, which resulted in empty documents
- Fixed default country search scope for sites
- Fixed resource caching for cloud sites with native OpenStack endpoints

[6.2.0] - 2019-06-14

Changed

- Populate VM images from site endpoints exposing native APIs (e.g. openstack) along with OCCI enabled ones
- Updated acceptable netfilter rules according to RFC 1123

Fixed

- Fixed organizations autocomplete list redirection bug
- Fixed bug related to missing organizations
- Fixed bug related to VA expiry dates

[6.1.15] - 2019-04-10

Changed

- Access to VO-wide image lists granted site administrators for sites with org.openstack.nova endpoints

[6.1.14] - 2019-01-25

Changed

- Added more warning messages and documentation links in continuous delivery UI to prevent user mistakes

Fixed

- Properly handle site images that are not provided under a VO wide image list

[6.1.13] - 2019-01-10

Fixed

- Fixed invalid report of expired VM versions in site details page

[6.1.12] - 2018-12-06

Fixed

- Fixed issues regarding base64 encoding of unicode and object types
- Fixed paging in RESTful API VO member/contact, etc resources
- Fixed invalid edit button on non-editable person profile tabs

[6.1.11] - 2018-11-22

Changed

- Improved internal server errors display
- Improved performance of openAIRE searching

Fixed

- Properly handle unicode characters in user input when creating a new user account
- Display short name for all organizations retrieved from openAIRE

7.1.2.2 7.1.2.2 VMOps dashboard

[1.3.9] - 2019-06-14

Added

- UI warnings related to VO constraints in supported VO list

[1.3.8] - 2019-06-03

Added

- Documentation for VO enrolment process

[1.3.7] - 2019-05-23

Fixed

- Disable topology/VM toolbox in UI immediately after an action is dispatched to infrastructure

[1.3.6] - 2019-05-16

Changed

- Updated obsolete argo.egi.eu status report URLs

[1.3.5] - 2019-05-15

Fixed

- Avoid storing obsolete images reported by site services

[1.3.4] - 2019-05-10

Added

- Support for VO blazarmonitoring.asi.it

[1.3.3] - 2019-03-21

Added

- Support for VO hidronav.eosc-hub.eu

[1.3.2] - 2019-03-15

Changed

- Simplified UI of VO quotas reports

Fixed

- Handle edge cases regarding VO resource usage calculation

[1.3.1] - 2019-03-14

Changed

- Revised display of contextualization logs
- Display current VO usage in VO quotas administrative panel

Fixed

- VO Quotas usage calculations and UI warnings

[1.3.0] - 2019-03-07

Added

- Support for predefined VO quotas per user

[1.2.3] - 2018-11-30

Added

- Support for VOs dih-voucher[01-30].eosc-hub.eu

[1.2.2] - 2018-11-06

Added

- Support for VO vo.clarin.eu

Changed

- Changelog format is now based in Keep a Changelog
- Revert connect-mongo package as newer connect-mongodb-session had connectivity issues

[1.2.1] - 2018-10-25

Changed

- Allow administrators to refresh users undeployed items by infrastructure
- Upgraded session storage

Fixed

- Fix bugs regarding unknown UI errors due to session mismanagement

7.1.2.3 VMOps service

[1.5.10] - 2019-07-09

Fixed

- Properly unset undeployment action when errors occur

[1.5.9] - 2019-06-20

Fixed

- Resource usage incompatibility issues with some mongodb instances
- Properly convert units of memory values retrieved from IM backend

[1.5.8] - 2019-05-23

Changed

- Reduced monitoring frequence of topologies and VMs from the infrastructure

[1.5.7] - 2019-03-14

Fixed

- Incompatible aggregation syntax for older versions of mongodb on resource usage api

[1.5.6] - 2019-03-07

Added

- Add API endpoint to query for resource usage from the VMOPs service per vo, service or user

7.1.2.4 InfoSys publisher

[1.3.3] - 2019-02-05

Changed

- Update third party dependencies to their current version

Fixed

- Allow graphql schema introspection to production instances

[1.3.2] - 2018-11-05

Changed

- Update third party dependencies to their current version
- Use package.json version value from graphql version resolver
- Clean up unused code

7.1.2.5 InfoSys MsgQ Listener

[0.2.2] - 2019-09-12

Fixed

- Handle missing attributes section of subscription message and extract such information from topic name

[0.2.1] - 2018-11-16

Changed

- Generate flat and tree json files for each site service endpoint
- Allow user to access separate site service endpoints from local service in the form of SITE_<SITE NAME>_ENDPOINT_<GOCDB ENDPOINT ID>

7.1.3 Future plans

- Provide support for OpenID Connect
- Extend the AppDB IS to support GLUE 2.1 schema
- Provide support for native APIs in VMOps dashboards
- Drop OCCI support from VMOps dashboard
- Development of the Endorser Dashboard
- Development of the Security Dashboard

7.2 GitLab

7.2.1 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	Function tests (webview, api) are running in test environment on local test instance
TRL	9

7.2.2 Release notes

1.7.3 - 2019-09-17:

Changed

- Update Gitlab to version 12.2.4
- Update Mattermost to version 5.14.2

1.7.2 - 2019-07-23:

Changed

- Update Mattermost to version 5.12.0

1.7.1 - 2019-06-27:

Changed

- Update Gitlab to version 12.0.0

1.7.0 - 2019-06-21:

Changed

- Update Gitlab to version 11.11.3
- Update Mattermost to version 5.12.0

1.6.1 - 2019-05-29:

Changed

- Update Gitlab to version 11.11

1.6.0 - 2019-05-11:

Changed

- Update Gitlab to version 11.10.4
- Update Mattermost to version 5.10.0

1.5.4 - 2019-04-20:

Changed

- Update Gitlab to version 11.10.1

1.5.3 - 2019-04-13:

Changed

- Update Gitlab to version 11.9.8

1.5.2 - 2019-03-28:

Changed

- Update Gitlab to version 11.9.1

1.5.1 - 2019-03-20:

Changed

- Add Data Privacy Statement for GitLab
- Add Data Privacy Statement for Mattermost

1.4.4 - 2019-03-19:

Changed

- Update Gitlab to version 11.8.2

1.4.3 - 2019-03-09:

Changed

- Update Gitlab to version 11.8.1

1.4.2 - 2019-02-22:

Changed

- Update Gitlab to version 11.7.5

1.4.1 - 2019-02-07:

Changed

- Update Gitlab to version 11.7.4

1.4.0 - 2019-02-02:

Changed

- Update Mattermost to version 5.7.0
- Update Gitlab to version 11.7

7.2.3 Future plans

We will continuously support an entire DevOps lifecycle for the developers and service owners. We will add more cloud resources for future usage and increase the data backup volumes and frequencies. We will keep track on GitLab and Mattermost official releases and provide up-to-date features.

7.3 EGI software repository

7.3.1 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.
TRL	9

7.3.2 Release notes

[2.0.7] - 2019-10-14

Fixed

- Restored proper RSS syndication for internal product releases (CAs, SAM)

7.3.3 Future plans

The integration of Jenkins Continuous Integration (CI) with the EGI software repository by the quality assurance team, mentioned in previous plans in D5.3, has been completed. Currently, the following actions are under evaluation:

- Provide a new front-end for the UMD / CMD and internal production software repositories, based on the AppDB portal codebase.
- Move from RT to some other system, such as JIRA or AMS, for the software provisioning process.

8 Roadmap

8.1 Identification, Authentication, Authorisation and Attribute Management

The roadmap of technical and policy-related alignment activities, which have been identified across the EOSC-hub AAI services, is maintained in the project wiki [R10]. The wiki page also includes the roadmap of integration activities among B2ACCESS, Check-in, and eduTEAMS. The subsections that follow provide the roadmaps of service enhancements which are specific to each EOSC-hub AAI service.

8.1.1 B2ACCESS

- Update of underlying software stack [Q2 2020]
- Release of group/Project management endpoint [Q2 2020]

8.1.2 Check-in

- Improve integration with EUDAT B2ACCESS [Q1 2020]
- Add support for retrieving Proxy certificates through SSH key information managed by the EGI Check-in COmanage Registry [Q1 2020]
- Scope-based active attribute value selection: This enhancement will allow OAuth2 clients to limit the values of specific claims based on the requested scopes [Q1 2020]
- Improve the identity linking user experience and interface [Q2 2020]
    - Improve linked identities panel by including localised friendly name & logo of user's IdP
    - Enable implicit identity linking
- Add support for (de-)provisioning and continuous update of user account information:
    - SCIM [Q4 2020]

8.1.3 eduTEAMS

- Upgrade to eduTEAMS v3 [Q1 2020]
- Step-up authentication service [Q1 2020]
- Enable Active Attribute Selection feature [Q2 2020]
- Integration with the Step-up Authentication Pilot Service [Q2 2020]
- New OpenID Connect Frontend [Q2 2020]
- Support for OIDC Federation specification [Q2 2020]

8.1.4 Perun

- New GUI [Q2 2020]
- Improved UX for the account linking [Q3 2020]
- Redesign workflow for account linking [Q3 2020]
- Performance optimization [Q4 2020]
- New user profile interface [Q3 2020]

- Improved integration with authentication proxies [Q4 2020]
- Pentesting [Q1 2021]
- Improved user documentation [Q3 2020]
- Automatization of operation process [Q4 2020]
- New roles and authorization module [Q2 2020]
- Improved process for the synchronization of users, attributes and group from external systems [Q3 2020]

8.1.5 WaTTS

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

8.1.6 MasterPortal

- Support high availability deployment [Q3 2020]

8.1.7 RCauth - Online CA

- Support high availability deployment to allow distributing the service geographically across the federated operators, i.e. GRNET, STFC, and Nikhef [Q1 2020]
- Production HA RCauth - monitoring, user documentation, performance metrics [Q2 2020]
- Compliance audit [Q3 2020], presented to IGTF for retention of certification and completion of tasks.

8.2 Marketplace and Order Management Tools

8.2.1 Marketplace

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

8.2.2 Service Portfolio Management Tool

2019

- Provide an api for the CMDBs (GOCDB and DMPT) to get list of approved the service_types [Q4 2019]
- Add In_Marketplace flag to Service Versions [Q1 2019]
- Adapt service model to support SDT v1.2 [Q3 2019]

2020

- Integrate with Marketplace [Q2 2020]
- Adapt service model to support SDT v2.0 [Q2 2020]

8.3 Integrated Business and Operations Support Systems

8.3.1 Operations Portal

- Integration with EOSC AAI [Q1, 2020]
- SLA Management Module in SOMBO [Q2, 2020]
    - For a given service order generate a document (or several documents) which will correspond to an agreement between the resource provider(s) and the customer.
    - The interface will provide different templates of documents depending on the type of resources.
- Add usage reports into the Service Order Management Back Office. [Q3,2020]
- Metrics module for EC [Q4,2020]

8.3.2 GOCDB

- Improve configuration management to ensure the long-term stability of the service [Q2,2020]
- Improvements and modification of “Reserved Scopes” handling in GOCDB [Q2,2020]
- Change in the underlying infrastructure of GOCDB to improve reliability. [Q2,2020]
- Creating new EOSC-Hub specific ServiceTypes automatically when they are added to the EOSC-Hub SPMT API. [Q2,2020]
- A second, configuration managed, production instance of GOCDB will be deployed behind our load balancer. [Q2,2020]
- The functionality of the Write API will be expanded to meet evolving use cases. [Q2,2020]
- EOSC-hub separate view under its own URL to show resources with the ‘EOSC-Hub’ scope tag applied, and we will use the current ServiceGroup functionality to represent EOSC-Hub's federated services [Q1,2020]

8.3.3 Data Project Management Tool

- Further enhancement of accounting records in StAR format [Q1, 2020]
- Migration to Plone 5.2 and Python 3 [Q2,2020]
- Connect DPMTs request handling to the EOSC order management via a message bus to be in line with the general switch to the AMS message bus for communication between services [Q1,2020]
- When collecting service information from SPMT: switch to SPMT API version 2 [Q2,2020]

8.3.4 Data Management Planning Tool

- Align the schema of EasyDMP with that of the RDA common DMP standard to demonstrate the interoperability between EasyDMP and openDMP by exporting plan from one tool to another. [Q2, 2020]
- Further services that make the data management plans machine actionable and verifiable will be developed as part of EOSC-HUB and interfaced to easyDMP and openDMP. [2020]
- Support local deployments of the eestore and extend the resources harvested (to include the SPMT/DPMT). [Q2,2020]

- To onboard the OpenDMP tool into the EOSC portfolio of services. [Q1,2020]
- Integration with DMPT and automatic procedure for update of data management plan based on the information provided in Marketplace order. [Q3, 2020]

8.3.5 SVMON

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

8.4 Monitoring, Accounting, Messaging, Security Tools

8.4.1 Accounting Repository

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

8.4.2 Accounting Portal

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

8.4.3 ARGO Monitoring

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

8.4.4 ARGO Messaging Service

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

- Support EGI Information System [2020]
- Support AppDB [2020]

8.4.5 Security Tools

8.4.5.1 Pakiti

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

8.4.5.2 Secant

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

8.5 Helpdesk Services and Tools

8.5.1 GGUS

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

8.5.2 EUDAT-RT

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

8.5.3 xGUS

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

8.6 Application store, Software Repositories

8.6.1 Application Database

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

8.6.2 GitLab

- Support and maintenance of entire DevOps cycle [2020]
- Increase resources for the instance from 6GB to 16GB [Q1, 2020]

8.6.3 EGI software repository

- Move from EGI SSO to EGI AAI authentication for admin instance [Q1, 2020]
- Provide a new front-end for the UMD / CMD and internal production software repositories, based on the AppDB portal codebase. [Q4, 2020]
- Move from RT to some other system, such as JIRA or AMS, for the software provisioning process. [Q4, 2020]

9 References

No	*Description/Link*
R1	https://www.eosc-hub.eu/catalogue
R2	https://keepachangelog.com
R3	https://github.com/postmanlabs/newman
R4	https://getpostman.com
R5	https://www.getpostman.com/docs/collections
R6	https://rt.egi.eu/rt/Dashboards/2636/GGUS-Requirements
R7	https://its.cern.ch/jira/browse/GGUS
R8	https://dashboard.appdb.egi.eu
R9	https://appdb-dev.marie.hellasgrid.gr/
R10	https://confluence.egi.eu/display/EOSC/AAI+Roadmap