

**EGI-Engage**

Infrastructure tests and best usage practices  
for life science service providers

D6.10

|  |  |
| --- | --- |
| **Date** | 31 May 2016 |
| **Activity** | SA2 |
| **Lead Partner** | CSC |
| **Document Status** | DRAFT |
| **Document Link** | https://documents.egi.eu/document/2802 |

Abstract

ELIXIR Competence Centre (CC) aims to bring the EGI resources, especially the EGI Federated Could, better available to the ELIXIR user community. This document sums up the experiences of those ELICIR CC members who are providing resources for EGI Federated Cloud and/or have utilized EGI resources for providing life science services.

**COPYRIGHT NOTICE**



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

**DELIVERY SLIP**

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

**DOCUMENT LOG**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Issue*** | ***Date*** | ***Comment*** | ***Author/Partner*** |
| **v.1** | 29/Apr/2016 | Document skeleton | G. Sipos / EGI.eu |
| **v.2** | 2/May/2016 | ToC | K. Mattila / CSC |
| **v.3** | 3/May/2016 | Corrected file | K. Mattila / CSC |
| **v.4** | 4/May/2016 | Restructuring after ELIXIR CC teleconference | G. Sipos / EGI.eu |
| **v.5** | 4/May/2016 | Initial text into Introduction, ECP description | G. Sipos / EGI.eu |
| **v.6** | 13/May/2016 | Some draft chapters added | K. Mattila / CSC |

**TERMINOLOGY**

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

**Contents**

1 Introduction 6

2 The ELIXIR Compute Platform; Role of service providers 7

3 Integration status and plans 9

3.1 CSC 9

3.2 EMBL-EBI 10

3.3 CESNET 10

3.4 CNRS 11

3.5 GRNET 11

3.6 SURFsara 12

3.7 JetStream 12

3.8 Other providers? 12

4 Integration guidelines and tips for service providers 13

4.1 Generic concepts and installation guidelines EGI 13

4.2 Installation guideline for OpenStack providers EGI 14

4.3 OpenStack-specific experiences, recommendations, tips EBI 15

4.4 Installation guideline for OpenNebula providers EGI 16

4.5 OpenNebula-specific experiences, recommendations, tips 17

4.6 Installation guideline for Synnefo providers EGI 18

4.7 Synnefo-specific experiences, recommendations, tips GRNET 18

4.8 JetStream integration experiences Indiana University 18

5 Report on AAI integration 19

5.1 Integration of ELIXIR AAI with EGI AAI proxy 19

5.2 Integration of GOCDB with the EGI AAI proxy 21

5.3 Integration of AppDB with the EGI AAI proxy 21

5.4 Integration of OpenStack with the EGI AAI proxy 22

Appendix I. User roles and permissions in GOCDB 24

**Executive summary**

ELIXIR[[1]](#footnote-1) is a pan-European research infrastructure in agreement between 17 European governments to build a sustainable European infrastructure for biological information, supporting life science research and its translation to medicine, agriculture, bioindustries and society.

EGI[[2]](#footnote-2) is a pan-European e-infrastructure that delivers integrated computing services to European researchers, driving innovation and enabling new solutions to answer the big questions of tomorrow.

The ELIXIR Competence Centre (CC) of the EGI-Engage project evaluates, adopts and promotes technologies and resources from EGI to the wider ELIXIR research community. This report is the second outcome of this effort. The document (1) describes the concept of the ELIXIR Compute Platform and responsibilities of service providers participating in it, (2) provides a status update about the completed, ongoing and planned integration of resources in this platform, and (3) presents integration guidelines for life science providers who are wishing to participate in this infrastructure.

The ELIXIR Compute Platform is a reference technical architecture to support a vast range of data analysis activities. EGI is currently contributing to the platform development with several services and technologies from EGI – all relating to the management and access of a cloud federation.

This document gives in overview of the state of EGI Federated Cloud integration of the ELIXIR CC members: Two sites (CESNET and GRNER) are already fully integrated, one site is in piloting state (EBI) and one preparing (CSC). Instructions for integrating new resources to EGI Federated Cloud are summed up and the experiences from the integration process are discussed.

A special focus is given to the recent work related to the integration of the Authentication and Authorization Infrastructures (AAI) of EGI and ELIXIR, as that will play a key role in the future activities.

# Introduction

ELIXIR[[3]](#footnote-3) is a pan-European research infrastructure in agreement between 17 European governments to build a sustainable European infrastructure for biological information, supporting life science research and its translation to medicine, agriculture, bioindustries and society.

EGI[[4]](#footnote-4) is a pan-European e-infrastructure that delivers integrated computing services to European researchers, driving innovation and enabling new solutions to answer the big questions of tomorrow.

Life science is a fast moving field. For the EGI services to become relevant and help keep European Life Sciences competitive globally, it is important to develop mechanisms that allow the research infrastructure to flexibly meet new challenges and respond to new scientific and technical developments.

The ELIXIR Competence Centre (CC) of the EGI-Engage project evaluates, adopts and promotes technologies and resources from EGI to the wider ELIXIR research community. This is achieved with an iterative approach:

1. Bringing together designated life science experts from ELIXIR and technical experts from EGI within the CC.
2. Identify life science use cases that could benefit from EGI services and could make big impact on ELIXIR and EGI communities. Analyse the e-infrastructure requirements of the use cases.
3. Implement the use cases as demonstrators based on EGI e-infrastructure services. Collaborate during implementation with relevant EGI and ELIXIR partners, such as the EUDAT[[5]](#footnote-5) to create a generic infrastructure, the ‘ELIXIR Compute Platform’ that can underpin demonstrators and production applications from/for the ELIXIR community.
4. Demonstrate and evaluate the implementations. Disseminate the experiences gained with the use cases towards ELIXIR, EGI and other relevant communities. Decide about the long-term adoption of EGI services within ELIXIR based on the pilot experiences.

This document is a deliverable produced by stage 3 of this process. It captures the goals, current status and plans for the ELIXIR Compute Platform, and provides guidelines for interested service providers to join the platform with cloud services.

The document was written by life science and e-infrastructure experts from ELIXIR and EGI who are brought together within the CC.

# The ELIXIR Compute Platform; Role of service providers

During 2015 the ELIXIR community – in collaboration with various e-infrastructures and other service providers – initiated the development of the reference architecture for ELIXIR, called the ‘ELIXIR Compute Platform’ (ECP). The prime role of the ECP is to support the use cases of the ELIXIR-EXCELERATE H2020 project, however, the platform is expected to serve other ELIXIR-related use cases from ELIXIR and other biomedical sciences Research Infrastructures. The demonstrator use cases of the CC (documented in M6.3) will also use this platform.

The need for an ELIXIR reference technical architecture was first discussed during a BioMedBridges e-Infrastructure workshop in May 2014, where reference was made to the MONARC report[[6]](#footnote-6) that formed the basis of the Tiered model that was initially adopted by WLCG community to serve the needs of High Energy Physics. Following on from work by the ELIXIR Authentication and Authorization Infrastructure (AAI), Storage and Cloud Task Forces to define a set of Technical Use Cases, a workshop was held in Amsterdam (12-13th March 2015) to discuss with representatives of ELIXIR nodes, European e-Infrastructures and other service providers, how the ELIXIR‑EXCELERATE Scientific Use Cases could be mapped onto the Technical Use Cases and thereby define the ELIXIR Compute Platform. Through a series of presentations and breakouts the technical aspects of the Scientific Use Cases were identified and mapped to a number of Technical Use Cases. As a result of these discussions, a number of recommendations have been made for technical solutions that together will provide an ELIXIR Compute Platform. The platform can not only support the ELIXIR-EXCELERATE Scientific Use Cases, but a vast range of other data analysis activities that will be found within the ELIXIR research community. Such as:

* Hosting portals that enable users to select and launch virtual machines onto an available cloud resource (e.g. for training activities).
* Hosting web tools that deploy a network of virtual machine images onto distributed cloud resources operated for ELIXIR users for large scientific analysis.
* Provisioning ‘Desktop as a Service’ where researchers are able to obtain a desktop image (e.g. BioLinux) in a cloud that they can use for their data analysis activities that is always on for their use.

The role of ELIXIR and the ELIXIR-EXCELERATE proposal is not to undertake middleware development. Instead the focus is on leveraging the investment that has already been made in services that can be integrated for our needs and steer future development priorities. Essentially, our role is to define a minimal ‘neck’ of an hourglass that ELIXIR Researchers and Application Developers can build upon and that ELIXIR Nodes and other infrastructure service providers can deploy and support. The ECP is envisaged to consist of the following service groups:

* Basic Identity Environment: authentication and authorization related infrastructure (“AAI”) to provide user identity and access management services[[7]](#footnote-7) for ‘ELIXIR infrastructure services’ (all other services). The basic ELIXIR AAI environment is available since the end of 2015 and further developments and refinements are coming during 2016.
* Core Enabling Infrastructure Services: provide capabilities to store and effectively transfer data (storage management and file transfer services). ELIXIR and EUDAT are working together in the EUDAT2020 project to identify, test and deploy services for this area.
* Basic Infrastructure Services: Cloud IaaS, Cloud Storage or HTC/HPC Cluster resource may be operated from within the ELIXIR community. ELIXIR is working with EGI in the context of the CC to implement this service area using technologies and know-how from the EGI Federated Cloud solution[[8]](#footnote-8). Priority focus is on cloud provisioning, and this is exactly in the main scope of this document: Providing guidelines for cloud resource providers about how to federate their services into the ELIXIR Compute Platform. Section 4 provides the related guidelines for service providers who are wishing to participate in the provisioning of the basic infrastructure services.
* Integrating Infrastructure Services: providing a federating structure that ensures a consistency of operation and behaviour across all resources and services of the ECP. ELIXIR and EGI are working together to implement this service area using technologies and know-how from the EGI Federated Operations solution[[9]](#footnote-9). The use of the GOCDB service registry together with the ELIXIR basic identity environment is the high priority integration activity in the CC. This would enable simple and reliable discovery of the integrated infrastructure services discoverable by life science users and applications. Section 5.2 of this report summarises the outcome of this work.
* Higher-Level Services: solutions that expand the platform to better serve specific use cases or use case categories. Competition among similar solutions is expected in this area. ELIXIR is working with EGI to bring in solutions into this area. High priority activity in the CC is integrating and using the EGI Virtual Machine/Virtual Appliances Marketplace[[10]](#footnote-10) in the ELIXIR Compute Platform. Section 5.3 of this report summarises the outcome of this work.

# Integration status and plans

## CSC

CSC provides an IaaS cloud service called cPouta for its customers (https://research.csc.fi/cpouta). This OpenStack based cloud service, funded by the Finnish Ministry of Culture and Education, allows users to launch their own virtual machines to a server environment running in the CSC computing center in Kajaani.

Currently the service contains nearly 3500 computing cores, used by over 200 computing projects. The majority of users are academic researchers working in Finland and requested access is granted by the CSC resource allocation board, but cPouta is also international collaboration projects, including some ELIXIR pilots. There are also some commercial users too, who buy the cPouta capacity directly from CSC.

As a member of EGI, CSC is interested in being part of the EGI Federated Cloud. However, as cPouta IaaS cloud is a production service that primarily supports Finnish researchers, joining the EGI Federated Cloud should not affect CSC's service level. In particular, EGI requirements of usage policies or maintenance work must have restricting impact on CSC's services.

The current key issues that need to be solved before CSC can formally join the EGI federated cloud are:

1. **Nova / Keystone integrations and compatibility with CSC's set-up**

It seems that these have improved lately, and now use more standard ways of integrating to OpenStack. The EGI's OpenStack integration will need to be tested by CSC to ensure compatibility with CSC's configuration. This also includes testing OpenStack release dependencies. This is to ensure that they work as expected, and that they don't cause unexpected issues with our other authentication and authorisation services. This also includes

testing OpenStack release dependencies.

1. **Architectural design**Previously, the Keystone LCMAPS integration broke CSC's design on stateless API nodes. This is (apparently) fixed, but CSC needs to ensure that there are no similar issues which break CSC's production architecture.
2. **Maintenance burden of supporting services**

The EGI Federated Cloud has supporting services like accounting, monitoring and service discovery. The integration and maintenance burden of these must be evaluated.

1. **User/group mapping issues**

The cPouta cloud uses project based access control where all resources are shared within a project. It appears that for the EGI Federated Cloud, users can only access their own resources. This and other possible differences in policies need to be resolved. The granularity of VO to OpenStack project mapping needs to be resolved.

1. **Quotas, accounting, billing**

The quotas, accounting and billing need to be resolved. How will this be integrated with CSC's billing system? (While the CSC system is primarily funded by the Finnish Ministry, outside access will be billed.)

1. **Timetable**

The production-level integration is not trivial, and this needs to be scheduled into CSC's development work. EGI's expectations need to be clarified. (Again, note that CSC already provides cloud services to an ELIXIR pilot.)

Operating an OpenStack cloud is resource intense. Adding extra integrations to a production OpenStack cloud increase the complexity of maintaining the cloud. To ensure the long term viability of this platform, CSC would like to be sure that it doesn't add undue burden to the maintenance and update process. Even once the above points have been considered, and potentially solved, more could arise.

## EMBL-EBI

What’s your status and plans for federating cloud and storage resources into the ELIXIR Compute Platform? What are the open questions (if any)?

## CESNET

CESNET operates a sizable national HPC infrastructure in Czech Republic providing resources to local academic communities, including cloud-based resources, various types of storage, and identity management services. On an international level, CESNET is a member of EGI (NGI\_CZ), as a resource provider and a technology provider, specifically in the context of EGI Federated Cloud.

As a resource provider, CESNET is fully integrated and offering the following cloud services compliant with EGI Federated Cloud:

* Virtual machine management via OCCI
* Accounting via APEL/SSM
* Information discovery via BDII
* Virtual machine image management via HEPiX vmcatcher/vmcaster
* AAI

CESNET supports appliances and virtual organizations required by the ELIXIR Compute platform.

As a technology provider, CESNET develops and maintains the following EGI Federated Cloud integration components and tools:

* OCCI components for virtual machine management (rOCCI-{core, api, cli, server})
* OpenNebula APEL connector (oneacct-export)
* OpenNebula Perun connector (fctf-perun)
* OpenNebula vmcatcher handler (itchy, nifty)
* OCCI monitoring probes for Nagios

## CNRS

What’s your status and plans for federating cloud and storage resources into the ELIXIR Compute Platform? What are the open questions (if any)?

## GRNET

GRNET operates Infrastructure as a Service ~okeanos via large datacenters (84 racks, 1200+ servers, 10000 Virtual Machines active, 5 Petabytes of storage). GRNET is also developing Synnefo, the cloud software for ~okeanos. The service was initially conceived and designed with the Greek Research and Academic community in mind, which comprises the natural user base of GRNET. Soon it became evident though that there is a wider potential and that this effort can be exploited in a broader environment. Towards this, ~okeanos has joined the EGI Federated Cloud activities with the aim to enhance its interoperability features and enable the offering of computing resources to the high-productivity federated infrastructure offered by EGI. ~Okeanos is fully integrated with EGI Federated Cloud and is offering the following services:

OCCI via the SNF-OCCI an implementation of the OCCI specification on top of synnefo’s API kamaki

CDMI via the SNF-CDMI an implementation of the CDMI specification on top of synnefo’s API kamaki

Accounting via the SNF-SSM implementation of the SSM accounting mechanism.

VM Image management via SNF-VMCATCHER.

GRNET supports the images required by ELIXIR CC such as Chipster. The plans for the next year is to update snf-occi to support OCCI 1.2 specification and to extend it capabilities.

## SURFsara

What’s your status and plans for federating cloud and storage resources into the ELIXIR Compute Platform? What are the open questions (if any)?

## JetStream

What’s your status and plans for federating cloud and storage resources into the ELIXIR Compute Platform? What are the open questions (if any)?

# Integration guidelines and tips for service providers

The ELIXIR Compute Platform uses the integration approach and integration technologies from the EGI Federated Cloud to establish the ‘basic infrastructure services’ layer (See section 2 for details). This section provides service deployment and configuration guidelines for cloud providers who are wishing to participate in the ELIXIR Compute Platform ‘basic infrastructure services’ layer. The section begins with a description of the EGI Federated Cloud concept, then provides integration information and tips for OpenStack, OpenNebula and Synnefo cloud service providers[[11]](#footnote-11).

## Generic concepts and installation guidelines

The EGI Federated Cloud integrates public and community clouds into a scalable computing platform for data and/or compute driven applications and services. Its architecture is based on the extension of the Cloud Management Frameworks deployed at the resource centres to provide a set of agreed uniform interfaces to the user communities and to the EGI Core infrastructure federator services. The federation of IaaS Resource Providers in EGI is built upon the extensive autonomy of resource centres in terms of ownership of the exposed resources. EGI does not mandate deploying any particular or specific Cloud Management Framework, providers should deploy the solution that fits best their individual needs whilst ensuring that the offered services implement the required interfaces.

EGI provides the services and technologies to extend the Cloud Management Frameworks (currently integration of OpenNebula, OpenStack and Synnefo are supported) to create federation of clouds. The cloud resource provider installation manual[[12]](#footnote-12) provides all the steps to deploy and configure the software components to support the federation on the supported Cloud Management Frameworks. Whenever possible these software components are designed and developed to not interfere the usual deployment of the cloud services but to use the already existing public interfaces and simply act as a client for those. The following services help to achieve the federation:

* **Federated AAI**, using X.509 proxy certificates and VOMS extensions with information on the VO of users. Integration with the new EGI AAI is currently under development.
* **Accounting**, usage information is collected via a secure messaging infrastructure in a centralised repository and displayed in a web portal where both individual users and communities can monitor their own resource/service usage across the whole federation.
* **Service Registry**, where providers register the different services offered to the federation.
* **Information Discovery**, so users and tools can retrieve a real-time view of the actual capabilities of the infrastructure.
* **VM Image catalogue and replication**. EGI AppDB provides a catalogue of Virtual Machine Images that encapsulate software appliances relevant for a given community. These images are automatically replicated to the local catalogues of the CMFs supporting the community.
* **Availability Monitoring**, to collect availability and reliability statistics about the providers that can be used to monitor SLAs and OLAs agreed with user communities and resource providers.
* **Standard Interfaces for IaaS**. OCCI and CDMI provide an interoperable interface across the different CMF, so users and applications can interact with the services offered with a single API.

Cloud providers joining the Federated Cloud follow EGI procedure to register and certify a Resource Centre (RC)[[13]](#footnote-13), which makes the EGI infrastructure aware of the new resources you offer, and takes care of validating and testing the behaviour of the services. In the context of the registration, the Resource Centre will become part of a Resource Infrastructure such as a National Grid Initiative (NGI), an EIRO, or a multi-country Resource Infrastructure.

## Installation guideline for OpenStack providers

Integration with of OpenStack providers on EGI’s FedCloud is supported on OpenStack releases from Havana to Mitaka (current release). The installation manual available at EGI’s wiki[[14]](#footnote-14) describe all the technical steps to perform this integration from a working OpenStack deployment. Which components must be installed and configured depends on the services to be offered: Keystone must be always available; if providing VM Management features (OCCI access or OpenStack access), then Nova, Cinder and Glance must be available; Swift needs to be available if providing object storage features.

The Figure shows the different components and their relation with the OpenStack and EGI services:

* Keystone-VOMS Authorization plugin allows users with a valid VOMS proxy to access the OpenStack deployment. This plugin requires modification of a regular Keystone installation.
* OpenStack OCCI Interface (ooi) translates between OpenStack API and OCCI. This is a WSGI application similar to other OpenStack services, it can be scaled horizontally to accommodate high loads.
* cASO collects accounting data from OpenStack using public APIs.
* SSM sends the records extracted by cASO to the central accounting database on the EGI Accounting service (APEL).
* BDII cloud provider registers the site configuration and description through the EGI Information System to facilitate service discovery.
* vmcatcher checks the EGI App DB for new or updated images that can be provided to the user communities (VO) supported and with the vmcatcher hooks (glancepush and OpenStack handler for vmcatcher) push updated images from to Glance, using Openstack Python API



There are two options for integration: using individual components or by using a configurable Virtual Appliance that encapsulates the components that just use the public APIs of OpenStack (marked as EGI integration tools in the image). Both options are detailed in the installation manual.

## OpenStack-specific experiences, recommendations, tips EBI

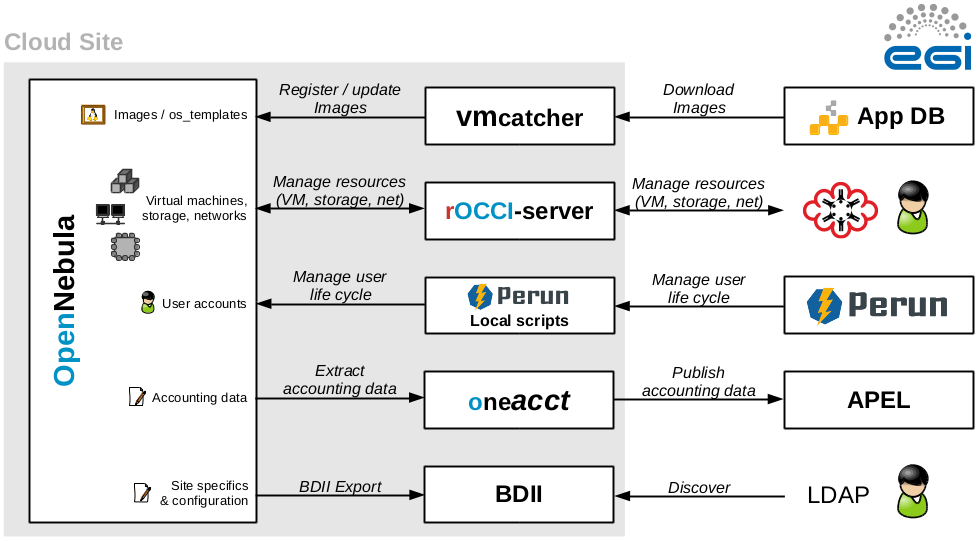
The deployment of EGI Federated Cloud integrator components has started at EMBL-EBI in late 2015. The goal was to federate the EMBL-EBI Openstack Kilo site into the EGI Federated Cloud, using the installation documentations[[15]](#footnote-15) that were available from EGI at that time. The first feedback from this experience was reported to EGI in the second half of February 2016. The feedback pointed out weaknesses in the installation manual and in the quality of some of the software components. The relevant EGI teams have implemented improvements both in the software and in the installation manuals. Based on the new versions EMBL-EBI successfully federated its OpenStack cloud site during April-May 2016. The site is based on OpenStack Kilo at the time of writing.

other info about the experiences of EBI?

## Installation guideline for OpenNebula providers

An EGI Cloud Site based on OpenNebula is an ordinary OpenNebula installation with some EGI-specific integration components. There are no additional requirements placed on internal site architecture. The installation manual available at EGI’s wiki[[16]](#footnote-16) describe all the technical steps to install the federation components on top of an OpenNebula deployment. CDMI storage endpoints are currently not supported for OpenNebula-based sites.

The Figure shows the components and their relation with OpenNebula and EGI services:



* rOCCI-server, which provides a standard OCCI interface. It translates between OpenNebula API and OCCI. It must be configured to use its opennebula backend, and to use voms for authentication.
* local perun scripts, which allow Perun[[17]](#footnote-17) to set up, block and remove user accounts from OpenNebula, thus managing the full life cycle of a user account.
* vmcatcher, which checks the EGI App DB for new or updated images that need to be supported on the site. It downloads images and registers them with OpenNebula, so that they can be used in resource instantiation. Vmcatcher configuration is explained bellow.
* oneacct scripts, which collect accounting data from OpenNebula and publish those into EGI's APEL instance. Oneacct configuration is explained at the FedCloud Accounting page.
* BDII cloud provider, which registers the site's configuration and description through the EGI Information System to facilitate service discovery.

## OpenNebula-specific experiences, recommendations, tips

OpenNebula-based service providers should follow the generic integration guidelines outlined in previous sections. In order to enable the ELIXIR Compute Platform, the following additional configuration is required:

1. Establish CA trust for proxy certificates issued by CILogon (https://snf-676811.vm.okeanos.grnet.gr/ca/demoroot.html)

$ cd /etc/grid-security/certificates

$ ls -la | grep Globus

lrwxrwxrwx 1 root root 22 Feb 25 09:54 93df451c.0 -> GlobusSimpleCaDemo.pem

-rw-r--r-- 1 root root 1931 Feb 25 09:53 GlobusSimpleCaDemo.pem

1. Enable VO 'vo.elixir-europe.org' locally

See https://wiki.egi.eu/wiki/HOWTO16#OpenNebula\_2

1. Enable propagations from Perun

Notify the Perun team via GGUS, state interest in 'vo.elixir-europe.org' being propagated to your EGI Federated Cloud site (provide site ID and endpoint URL).

1. Subscribe to 'vo.elixir-europe.org' VO-wide image list

See https://wiki.appdb.egi.eu/main:guides:vmcatcher\_site\_setup

After the first successful propagation from Perun (user accounts) and AppDB (virtual appliances), your site will be a fully functional member of the ELIXIR Compute Platform.

## Installation guideline for Synnefo providers

An EGI Cloud Site based on Synnefo[[18]](#footnote-18) is an ordinary Synnefo installation with some EGI-specific integration components. There are no additional requirements placed on internal site architecture. You will need however to install the following extra services.

* SNF-OCCI[[19]](#footnote-19): Which is an an implementation of OCCI 1.1 (OCCI 1.2 support will be available shortly) as a bridge to kakaki, synnefo cli.
* ASTAVOMS[[20]](#footnote-20): is the extension to synnefos astakos authentication services that handles a pool of user accounts to that are bind to a user authenticated via VOMS.
* SNF-CDMI[[21]](#footnote-21): Which is an implementation of CDMI Spec on top of pithos ~Okeanos storage service.
* SNF-SSM[[22]](#footnote-22): Which is a script that publishes to apel ssm usage records.
* SNF-VMCATCHER[[23]](#footnote-23): Which is the implementation of vmcatcher to use kakaki and snf-image to import images on your Synnefo installation.

Please note that astavoms is required for both SNF-OCCI and SNF-CDMI to work as they redirect to that service to authenticate a user.

## Synnefo-specific experiences, recommendations, tips

Synnefo does not have any specific requirements or recommendations besides that we do not support VMs with Logical Volumes.

# Report on AAI integration

This subsection provides details about the integration activities that were performed by EGI and the ELIXIR AAI Task Force to integrate EGI services with the ELIXIR Authentication-Authorisation Infrastructure (AAI). The AAI integration was implemented through the recently released EGI AAI proxy service[[24]](#footnote-24). The GOCDB service registry, and the AppDB Virtual Machine Image catalogue were selected as priority services to conduct the integration. Besides these OpenStack was also integrated with the EGI AAI proxy.

These integrations enable members of the ELIXIR Community to interact with GOCDB, AppDB and OpenStack resources using their ELIXIR user identities:

* In GOCDB these ELIXIR service providers can register and manage the registration of basic infrastructure resources (cloud and storage).
* In AppDB ELIXIR application developers can register Virtual Machine Images and Virtual Appliances for publishing these on the ELIXIR cloud sites and for sharing these with the broader life science community.
* In OpenStack ELIXIR members can instantiate applications from the pre-deployed Virtual Machine Images and Virtual Appliances.

The next subsections provides details on how the integration was achieved and what are the next steps.

## Integration of ELIXIR AAI with EGI AAI proxy

The ‘EGI AAI proxy’ is a new service in the EGI service portfolio which enables access to EGI services and resources with federated authentication mechanisms. Specifically, the proxy service is operated as a central hub between federated Identity Providers (IdPs) residing ‘outside’ of the EGI network of services, and Service Providers (SPs) that are part of EGI. The main advantage of this design principle is that all entities need to establish and maintain technical and trust relation only to a single entity, the EGI AAI proxy, instead of managing N-to-M relationships. The proxy acts as a Service Provider towards the Identity Providers and as an Identity Provider towards the Service Providers.

Using the EGI AAI proxy, users are able to authenticate with the credentials provided by the IdP of their Home Organisation through eduGAIN, as well as using social identity providers, eGOV IDs, or other selected external identity providers. To achieve this, the EGI AAI has built-in support for SAML, OpenID Connect and OAuth2 providers and already enables user logins through Facebook, Google, LinkedIn, and ORCID. In addition to serving as an authentication proxy, the EGI AAI provides a central Discovery Service (Where Are You From – WAYF) for users to select their preferred IdP.

The EGI AAI proxy is also responsible for aggregating user attributes originating from various authoritative sources (IdPs and attribute provider services) and delivering them to the connected EGI service providers in a harmonised and transparent way. Service Providers can use the received attributes for authorisation purposes, i.e. deciding what the user is allowed to use/do with the service. The EGI services require a minimum set of attributes from the EGI AAI proxy about the user to grant access[[25]](#footnote-25).

Within ELIXIR the ELIXIR AAI service operates as both an IdP and attribute provider service. It’s assumed that this service will manage user accounts and personal attributes for every ELIXIR user. During the last months the EEGI AAI proxy has been integrated with the ELXIR AAI with the goal to enable members of the ELIXIR Community access EGI services. Two EGI service – the GOCDB service registry and the AppDB Virtual Machine marketplace – were chosen as priority services for the ELIXIR integration. The integration work was achieved by connecting the SP proxy element of the EGI AAI proxy with the IdP proxy of the ELIXIR AAI with exchanging their SAML metadata in XML format.

The typical Single Sign-On (SSO) flow in the integrated system begins with the ELIXIR user accessing an EGI application (GOCDB or AppDB) through a web browser (SP-initiated SSO). Since the user is not logged in at the SP yet, the SP sends the user to the EGI IdP proxy to authenticate. The user is then redirected to the EGI central Discovery Service page where he/she is able to select to authenticate at ELIXIR. This results in a SAML authentication request from the EGI AAI proxy to the ELIXIR AAI (it’s IdP proxy component). Compliance of the EGI SP proxy with the GÉANT Data Protection Code of Conduct (CoCo) and the REFEDS Research and Scholarship (R&S) allows the ELIXIR AAI IdP proxy to release the minimum set of attributes required for a user to make use of the EGI service.

The released attribute set includes an opaque (eduPersonalUniqueId), as well as a username-based (eduPersonPrincipalName) user identifier scoped at elixir-europe.org. The first name (givenName), surname (sn) and email (mail) of the user are also provided. To indicate the set of rights to specific EGI resources, the ELIXIR IdP proxy releases an eduPersonEntitlement attribute. This is a multi-valued attribute, with each value formatted as a URI. The structure of the value itself however, is based on an agreement between ELXIR and EGI, since there are currently no commonly accepted standards or recommendations regarding the representation of entitlements. The eduPersonEntitlement content is still under discussion, finalisation is expected by the end of May.

The ELIXIR IdP builds an assertion containing the attributes above, which is sent to the SP proxy component of the EGI AAI proxy. Based on the authentication method selected by the user, the EGI proxy assigns a Level of Assurance (LoA)[[26]](#footnote-26), which is conveyed to the SP through the eduPersonAssurance attribute and the Authentication Context Class of the SAML authentication response. EGI AAI currently distinguishes between three LoA levels, namely, Low, Substantial and High. Some EGI SPs have been configured to provide limited access (or not to accept at all) credentials with the Low LoA. Details regarding LoA levels in case of GOCDB and AppDB are reported in the next subsections.

## Integration of GOCDB with the EGI AAI proxy

GOCDB has been integrated with the EGI AAI proxy. This allows users without a client x509 certificate to access GOCDB provided the user authenticates to the AAI proxy using an authentication scheme that provides an adequate level of assurance (LoA). As a central configuration management database, GOCDB requires the highest level of assurance. For example, if the user authenticates to the ProxyIdP using a scheme that provides a low or medium level of assurance such as social-media/Facebook, then access to GOCDB is denied. Conversely, if a project integrates a trusted identity provider with the ProxyIdP where the user authenticates using a scheme that provides a high LoA (e.g. institutional credentials), access is granted. During the login process, the LoA category that is assigned to the user's authenticated session (e.g. low, substantial, high) is communicated to the GOCDB. The ELIXIR AAI IdP provides the highest level of assurance to GOCDB.

Based on the provided assurance level, GOCDB can make its own internal authorisation decisions. If a user is granted access, they use the existing GOCDB role mechanisms to request roles and permissions. The list of available roles, with their permissions is provided in Appendix 1. There is no automatic mapping between ELIXIR roles and GOCDB roles.

* 1. User logs in to GOCDB service registry with ELIXIR account (<http://goc.egi.eu>)
  2. User requests a role. The request is passed to the existing users who already own the necessary roles to approve or reject the role request. Currently Steven Newhouse from EBI and Miroslav Ruda from CESNET who have roles over the ELIXR group. (Once this initial community admin group is established within GOCDB by the GOCDB admin, the group can subsequently self-manage their user memberships.)
  3. User is granted with the approved role at next login, and can perform authorised operations.

## Integration of AppDB with the EGI AAI proxy

EGI AppDB is planned to be used as a marketplace of Virtual Machine Images (VMIs) within the ELIXIR Compute platform. A user can have three roles when accessing the EGI AppDB marketplace:

* Visitor: Can browse publicly visible VMIs, can download them for local use. Visitors do not have to login.
* Member of a scientific community: Can register new VMIs and VMI versions in the marketplace and (optionally) can submit these to community coordinator for inclusion in the community image list. Community members have to login to AppDB and must have user attribute that express affiliation to the community.
* Coordinator of a scientific community: Can add VMIs to the community image list to trigger the replication of these VMIs to the cloud sites that support the community. Community image list includes VMs that are of high relevance to the scientific community. Community coordinators have to login to AppDB and must have attributes that express affiliation to a community and coordinator role within that community.

The goal of the AppDB–ELIXIR AAI integration was to enable authorized access to the marketplace for members of the ELIXIR community - i.e. for those possessing ELIXIR accounts.

The integration of AppDB with the EGI ProxyIdP has been completed, so AppDB can login and authorise users coming through the EGI AAI proxy. Authorization of user actions is based on relevant entitlements returned by the EGI AAI proxy (including LoA entitlement).

The integration is currently stalled on waiting for the agreement on the normalized entitlement schema between the ELIXIR AAI and EGI AAI proxy. Once entitlement normalization is complete, the EGI AAI subsystem of AppDB will be able to move to production and eventually expand the existing authentication and authorization methods (EGI SSO, x.509) with new options.

## Integration of OpenStack with the EGI AAI proxy

Until recently OpenStack resources of the EGI Federated Cloud were able to authenticate and authorize users solely through X.509 proxy certificates. This prevented users without a client X.509 certificate to interact with the providers. The latest versions of the OpenStack identity service (Keystone) now includes support for federated users: Keystone can act as a Service Provider (SP) that consumes identity properties issued by an external Identity Provider, such as SAML assertions or OpenID Connect claims. The OpenStack web dashboard (Horizon) has introduced also support for this kind of authentication and authorisation. Based on this new OpenStack feature EGI has connected OpenStack with the EGI AAI proxy. The integration is achieved with a new configuration of the Keystone federation that uses EGI AAI as a SAML IdP. Detailed instructions are available in the OpenStack guides[[27]](#footnote-27).

The below screenshot shows the SAML-enabled OpenStack dashboard with its drop down menu of available authentication providers. When selecting the egi.eu IdP proxy option, user will be redirected to the EGI AAI proxy and can follow the process described in section 5.1 to authenticate with an ELIXIR account.



Figure 1. EGI AAI IdP proxy configured in OpenStack

Site administrators need to set up the rules that map the attributes released from the EGI AAI proxy to local OpenStack identity objects. There are many ways to setup and combine these rules. For the EGI integration the following objects are used:

* eduPersonalUniqueId, is mapped to the user id in Keystone.
* eduPersonEntitlement defines the OpenStack groups the user is allowed to access,
* Level of Assurance may restrict grant access to users with the desired LoA

Once the eduPersonEntitlement contents are agreed, recommended mappings will be provided for administrators to easily integrate their resources. Users authenticated through this mechanism can be managed by the OpenStack administrator as any other user.

1. User roles and permissions in GOCDB

In GOCDB, users request Roles over domain objects such as Projects, NGIs, Sites and ServiceGroups. A Role enables Actions on target objects (often, the target is the same as the domain object). Some Roles allow actions over different targets.

The Role-Action mapping matrix is shown below. The matrix was copied from GOCDB page <https://goc.egi.eu/portal/index.php?Page_Type=View_Role_Action_Mappings>.

**ServiceGroup Roles**

| **RoleType** | **Action** | **On (Target of Action)** |
| --- | --- | --- |
| Service Group Administrator | ACTION\_EDIT\_OBJECT | ServiceGroup |
| Service Group Administrator | ACTION\_GRANT\_ROLE | ServiceGroup |
| Service Group Administrator | ACTION\_REJECT\_ROLE | ServiceGroup |
| Service Group Administrator | ACTION\_REVOKE\_ROLE | ServiceGroup |

**Project Roles**

| **RoleType** | **Action** | **On (Target of Action)** |
| --- | --- | --- |
| COD Staff | ACTION\_EDIT\_OBJECT | Project |
| COD Staff | ACTION\_GRANT\_ROLE | Project |
| COD Staff | ACTION\_REJECT\_ROLE | Project |
| COD Staff | ACTION\_REVOKE\_ROLE | Project |
| COD Staff | ACTION\_GRANT\_ROLE | Ngi |
| COD Staff | ACTION\_REJECT\_ROLE | Ngi |
| COD Staff | ACTION\_REVOKE\_ROLE | Ngi |
| COD Staff | ACTION\_SITE\_EDIT\_CERT\_STATUS | Site |
| COD Administrator | ACTION\_EDIT\_OBJECT | Project |
| COD Administrator | ACTION\_GRANT\_ROLE | Project |
| COD Administrator | ACTION\_REJECT\_ROLE | Project |
| COD Administrator | ACTION\_REVOKE\_ROLE | Project |
| COD Administrator | ACTION\_GRANT\_ROLE | Ngi |
| COD Administrator | ACTION\_REJECT\_ROLE | Ngi |
| COD Administrator | ACTION\_REVOKE\_ROLE | Ngi |
| COD Administrator | ACTION\_SITE\_EDIT\_CERT\_STATUS | Site |
| EGI CSIRT Officer | ACTION\_EDIT\_OBJECT | Project |
| EGI CSIRT Officer | ACTION\_GRANT\_ROLE | Project |
| EGI CSIRT Officer | ACTION\_REJECT\_ROLE | Project |
| EGI CSIRT Officer | ACTION\_REVOKE\_ROLE | Project |
| EGI CSIRT Officer | ACTION\_GRANT\_ROLE | Ngi |
| EGI CSIRT Officer | ACTION\_REJECT\_ROLE | Ngi |
| EGI CSIRT Officer | ACTION\_REVOKE\_ROLE | Ngi |
| EGI CSIRT Officer | ACTION\_SITE\_EDIT\_CERT\_STATUS | Site |
| Chief Operations Officer | ACTION\_EDIT\_OBJECT | Project |
| Chief Operations Officer | ACTION\_GRANT\_ROLE | Project |
| Chief Operations Officer | ACTION\_REJECT\_ROLE | Project |
| Chief Operations Officer | ACTION\_REVOKE\_ROLE | Project |
| Chief Operations Officer | ACTION\_GRANT\_ROLE | Ngi |
| Chief Operations Officer | ACTION\_REJECT\_ROLE | Ngi |
| Chief Operations Officer | ACTION\_REVOKE\_ROLE | Ngi |
| Chief Operations Officer | ACTION\_SITE\_EDIT\_CERT\_STATUS | Site |

**NGI Roles**

| **RoleType** | **Action** | **On (Target of Action)** |
| --- | --- | --- |
| NGI Operations Manager | ACTION\_EDIT\_OBJECT | Ngi |
| NGI Operations Manager | ACTION\_NGI\_ADD\_SITE | Ngi |
| NGI Operations Manager | ACTION\_GRANT\_ROLE | Ngi |
| NGI Operations Manager | ACTION\_REJECT\_ROLE | Ngi |
| NGI Operations Manager | ACTION\_REVOKE\_ROLE | Ngi |
| NGI Operations Manager | ACTION\_EDIT\_OBJECT | Site |
| NGI Operations Manager | ACTION\_SITE\_ADD\_SERVICE | Site |
| NGI Operations Manager | ACTION\_SITE\_DELETE\_SERVICE | Site |
| NGI Operations Manager | ACTION\_GRANT\_ROLE | Site |
| NGI Operations Manager | ACTION\_REJECT\_ROLE | Site |
| NGI Operations Manager | ACTION\_REVOKE\_ROLE | Site |
| NGI Operations Manager | ACTION\_SITE\_EDIT\_CERT\_STATUS | Site |
| NGI Operations Deputy Manager | ACTION\_EDIT\_OBJECT | Ngi |
| NGI Operations Deputy Manager | ACTION\_NGI\_ADD\_SITE | Ngi |
| NGI Operations Deputy Manager | ACTION\_GRANT\_ROLE | Ngi |
| NGI Operations Deputy Manager | ACTION\_REJECT\_ROLE | Ngi |
| NGI Operations Deputy Manager | ACTION\_REVOKE\_ROLE | Ngi |
| NGI Operations Deputy Manager | ACTION\_EDIT\_OBJECT | Site |
| NGI Operations Deputy Manager | ACTION\_SITE\_ADD\_SERVICE | Site |
| NGI Operations Deputy Manager | ACTION\_SITE\_DELETE\_SERVICE | Site |
| NGI Operations Deputy Manager | ACTION\_GRANT\_ROLE | Site |
| NGI Operations Deputy Manager | ACTION\_REJECT\_ROLE | Site |
| NGI Operations Deputy Manager | ACTION\_REVOKE\_ROLE | Site |
| NGI Operations Deputy Manager | ACTION\_SITE\_EDIT\_CERT\_STATUS | Site |
| NGI Security Officer | ACTION\_EDIT\_OBJECT | Ngi |
| NGI Security Officer | ACTION\_NGI\_ADD\_SITE | Ngi |
| NGI Security Officer | ACTION\_GRANT\_ROLE | Ngi |
| NGI Security Officer | ACTION\_REJECT\_ROLE | Ngi |
| NGI Security Officer | ACTION\_REVOKE\_ROLE | Ngi |
| NGI Security Officer | ACTION\_EDIT\_OBJECT | Site |
| NGI Security Officer | ACTION\_SITE\_ADD\_SERVICE | Site |
| NGI Security Officer | ACTION\_SITE\_DELETE\_SERVICE | Site |
| NGI Security Officer | ACTION\_GRANT\_ROLE | Site |
| NGI Security Officer | ACTION\_REJECT\_ROLE | Site |
| NGI Security Officer | ACTION\_REVOKE\_ROLE | Site |
| NGI Security Officer | ACTION\_SITE\_EDIT\_CERT\_STATUS | Site |
| Regional Staff (ROD) | ACTION\_EDIT\_OBJECT | Ngi |
| Regional Staff (ROD) | ACTION\_EDIT\_OBJECT | Site |
| Regional Staff (ROD) | ACTION\_SITE\_ADD\_SERVICE | Site |
| Regional Staff (ROD) | ACTION\_SITE\_DELETE\_SERVICE | Site |
| Regional First Line Support | ACTION\_EDIT\_OBJECT | Ngi |
| Regional First Line Support | ACTION\_EDIT\_OBJECT | Site |
| Regional First Line Support | ACTION\_SITE\_ADD\_SERVICE | Site |
| Regional First Line Support | ACTION\_SITE\_DELETE\_SERVICE | Site |

**Site Roles**

| **RoleType** | **Action** | **On (Target of Action)** |
| --- | --- | --- |
| Site Administrator | ACTION\_EDIT\_OBJECT | Site |
| Site Administrator | ACTION\_SITE\_ADD\_SERVICE | Site |
| Site Administrator | ACTION\_SITE\_DELETE\_SERVICE | Site |
| Site Security Officer | ACTION\_EDIT\_OBJECT | Site |
| Site Security Officer | ACTION\_SITE\_ADD\_SERVICE | Site |
| Site Security Officer | ACTION\_SITE\_DELETE\_SERVICE | Site |
| Site Security Officer | ACTION\_GRANT\_ROLE | Site |
| Site Security Officer | ACTION\_REJECT\_ROLE | Site |
| Site Security Officer | ACTION\_REVOKE\_ROLE | Site |
| Site Operations Deputy Manager | ACTION\_EDIT\_OBJECT | Site |
| Site Operations Deputy Manager | ACTION\_SITE\_ADD\_SERVICE | Site |
| Site Operations Deputy Manager | ACTION\_SITE\_DELETE\_SERVICE | Site |
| Site Operations Deputy Manager | ACTION\_GRANT\_ROLE | Site |
| Site Operations Deputy Manager | ACTION\_REJECT\_ROLE | Site |
| Site Operations Deputy Manager | ACTION\_REVOKE\_ROLE | Site |
| Site Operations Manager | ACTION\_EDIT\_OBJECT | Site |
| Site Operations Manager | ACTION\_SITE\_ADD\_SERVICE | Site |
| Site Operations Manager | ACTION\_SITE\_DELETE\_SERVICE | Site |
| Site Operations Manager | ACTION\_GRANT\_ROLE | Site |
| Site Operations Manager | ACTION\_REJECT\_ROLE | Site |
| Site Operations Manager | ACTION\_REVOKE\_ROLE | Site |

1. <http://www.elixir-europe.org/> [↑](#footnote-ref-1)
2. <http://www.egi.eu/> [↑](#footnote-ref-2)
3. <http://www.elixir-europe.org/> [↑](#footnote-ref-3)
4. <http://www.egi.eu/> [↑](#footnote-ref-4)
5. <http://www.eudat.eu/> [↑](#footnote-ref-5)
6. It is worth noting that the MONARC report is now considered outdated as following the initial experience of running the WLCG and the advances in the capability of the international networks, an evolved technical architecture is now being established that is less hierarchical in its data flows. [↑](#footnote-ref-6)
7. ELIXIR AAI – Requirements and Design: <https://docs.google.com/document/d/1CMY1np3GyvPD8LcKvXljXcRO04V2zu3n_Jcg19jgNOw/edit> [↑](#footnote-ref-7)
8. <https://www.egi.eu/solutions/fed-cloud/index.html> [↑](#footnote-ref-8)
9. <https://www.egi.eu/solutions/fed-ops/index.html> [↑](#footnote-ref-9)
10. <https://appdb.egi.eu/browse/cloud> [↑](#footnote-ref-10)
11. OpenStack, OpenNebula and Synnefo are those cloud management frameworks for which integration components already exists. Integrator components can be developed for additional cloud system if needed. [↑](#footnote-ref-11)
12. https://wiki.egi.eu/wiki/MAN10 [↑](#footnote-ref-12)
13. https://wiki.egi.eu/wiki/PROC09\_Resource\_Centre\_Registration\_and\_Certification [↑](#footnote-ref-13)
14. https://wiki.egi.eu/wiki/MAN10#Integrating\_OpenStack [↑](#footnote-ref-14)
15. <https://wiki.egi.eu/wiki/Federated_Cloud_resource_providers_support#Join_as_a_Resource_Provider> [↑](#footnote-ref-15)
16. https://wiki.egi.eu/wiki/MAN10#Integrating\_OpenNebula [↑](#footnote-ref-16)
17. https://perun.metacentrum.cz/ [↑](#footnote-ref-17)
18. https://www.synnefo.org [↑](#footnote-ref-18)
19. <https://github.com/grnet/snf-occi> [↑](#footnote-ref-19)
20. [↑](#footnote-ref-20)
21. <https://github.com/grnet/snf-cdmi> [↑](#footnote-ref-21)
22. <https://github.com/grnet/snf-ssm> [↑](#footnote-ref-22)
23. https://github.com/grnet/snf-vmcatcher [↑](#footnote-ref-23)
24. The EGI AAI Proxy service was developed by the JRA1.1 task of EGI-Engage: <https://wiki.egi.eu/wiki/EGI-Engage:WP3#TASK_JRA1.1_Authentication_and_Authorisation_Infrastructure> [↑](#footnote-ref-24)
25. The required attributes are eduPersonalUniqueId and the username-based eduPersonPrincipalName user identifier (scoped at [elixir-europe.org](http://elixir-europe.org) in case of ELIXIR). [↑](#footnote-ref-25)
26. LoA expresses the ability to determine, with some level of certainty, that the electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity. [↑](#footnote-ref-26)
27. <http://docs.openstack.org/developer/keystone/federation/federated_identity.html> [↑](#footnote-ref-27)