EGI-InSPIRE

EGI FEDERATED CLOUD BLUEPRINT V2

EU MILESTONE: MS521

Document identifier:	EGI-InSPIRE-MS521-final.docx
Date:	**16/06/2014**
Activity:	**SA2**
Lead Partner:	**EGI.eu**
Document Status:	**FINAL**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/2091

Abstract

This milestone document provides background information on the activities on the EGI Federated Cloud Task over PY4 and details of the integration work carried out over the past 6-month development cycle. This includes how the three classes of actors – the users, resource providers and technology providers – have contributed to the various activities. The document also has a section on the method by which new participants can join the federated cloud, what is required and expected of them.

The delivery of this milestone was postponed from PM46 to PM48 with project amendment n.3 in order to report on the preparation to the production phase of the EGI Cloud Infrastructure Platform taking into account the developments of the cloud-related mini-projects conducted in SA4.



I. COPYRIGHT NOTICE

II. DELIVERY SLIP

	Name	Partner/Activity	Date
From	David Wallom/Michel Drescher	OeRC/EGI.eu, SA2	12-06-2014
Reviewed by	**Moderator:** S. Andreozzi **Reviewers:** T. Ferrari	EGI.eu/NA2 EGI.eu/SA1	13-06-2014
Approved by	**AMB & PMB**		15-06-2014

III. DOCUMENT LOG

Issue	Date	Comment	Author/Partner
1	09/06/14	First draft based on MS520	David Wallom, UOXF
3	12/06/14	AMB review revision	Michel Drescher, EGI.eu

IV. APPLICATION AREA

This document is a formal deliverable for the European Commission, applicable to all members of the EGI-InSPIRE project, beneficiaries and Joint Research Unit members, as well as its collaborating projects.

V. DOCUMENT AMENDMENT PROCEDURE

Amendments, comments and suggestions should be sent to the authors. The procedures documented in the EGI-InSPIRE "Document Management Procedure" will be followed: https://wiki.egi.eu/wiki/Procedures

VI. TERMINOLOGY

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



VII. PROJECT SUMMARY

To support science and innovation, a lasting operational model for e-Science is needed – both for coordinating the infrastructure and for delivering integrated services that cross national borders.

The EGI-InSPIRE project will support the transition from a project-based system to a sustainable pan-European e-Infrastructure, by supporting 'grids' of high-performance computing (HPC) and high-throughput computing (HTC) resources. EGI-InSPIRE will also be ideally placed to integrate new Distributed Computing Infrastructures (DCIs) such as clouds, supercomputing networks and desktop grids, to benefit user communities within the European Research Area.

EGI-InSPIRE will collect user requirements and provide support for the current and potential new user communities, for example within the ESFRI projects. Additional support will also be given to the current heavy users of the infrastructure, such as high energy physics, computational chemistry and life sciences, as they move their critical services and tools from a centralised support model to one driven by their own individual communities.

The objectives of the project are:

1. The continued operation and expansion of today's production infrastructure by transitioning to a governance model and operational infrastructure that can be increasingly sustained outside of specific project funding.
2. The continued support of researchers within Europe and their international collaborators that are using the current production infrastructure.
3. The support for current heavy users of the infrastructure in earth science, astronomy and astrophysics, fusion, computational chemistry and materials science technology, life sciences and high energy physics as they move to sustainable support models for their own communities.
4. Interfaces that expand access to new user communities including new potential heavy users of the infrastructure from the ESFRI projects.
5. Mechanisms to integrate existing infrastructure providers in Europe and around the world into the production infrastructure, so as to provide transparent access to all authorised users.
6. Establish processes and procedures to allow the integration of new DCI technologies (e.g. clouds, volunteer desktop grids) and heterogeneous resources (e.g. HTC and HPC) into a seamless production infrastructure as they mature and demonstrate value to the EGI community.

The EGI community is a federation of independent national and community resource providers, whose resources support specific research communities and international collaborators both within Europe and worldwide. EGI.eu, coordinator of EGI-InSPIRE, brings together partner institutions established within the community to provide a set of essential human and technical services that enable secure integrated access to distributed resources on behalf of the community.

The production infrastructure supports Virtual Research Communities (VRCs) – structured international user communities – that are grouped into specific research domains. VRCs are formally represented within EGI at both a technical and strategic level.

VIII. EXECUTIVE SUMMARY

This milestone document summarises the activities of the EGI Federated Cloud conducted in task TSA2.6 over PY4. Activities are coordinated by a steering panel, and conducted multiple representatives of the three main stakeholders: Resource Providers, Technology Providers, and User Communities. Each member is expected to actively contribute as their individual commitment allows, ranging from best effort to partially funded effort coming from a variety of sources.

The activities contribute to and are aligned with a general architecture revision in EGI towards a platform-oriented architecture. The EGI Cloud Infrastructure Platform is the architectural incarnation of the activities in this Task, where Resource Providers are free in their choice of Cloud Management Frameworks (in alignment with the Cloud Computing paradigms) for as long as they are abiding by the federation's requirements. Different levels of federation are possible, depending on the needs of the user communities supported; the minimum level of federation requires the conformance to EGI policies and the adoption of federated AAI.

This model of *abstract Cloud Management Framework subsystems* allows architecting a scalable Cloud Infrastructure Platform without entangling its stakeholders in too many dependencies.

The federation requirements mainly consider services exposed to the consuming research communities, and the details of the back-end integration with the EGI Core Infrastructure Platform.

- Supporting the use cases of the Federated Cloud consumers, three core management open standard interfaces are provided: VM Management using *OCCI*, Data Management using *CDMI*, and Information Discovery using *LDAP and GLUE2*.
- Federated AAI is based on x509 Digital Certificates and SAML formatted assertions representing user authorisation decisions.
- Accounting is based on the EGI's accounting infrastructure and an extension of the OGF UR specification.
- Monitoring is based on the EGI's Service Availability Monitoring infrastructure and service registration in EGI's central service registry.

The work of the EGI Federated Cloud Task and definition of the EGI Cloud Infrastructure Platform is driven by 10 scenarios. This document provides summaries of the integration activities pertinent to Cloud Management Frameworks that have over the period of the activity been deployed in the Task's test bed (in no particular order: OpenNebula, OpenStack, StratusLab, WNoDeS and Synnefo) to meet the defined scenarios. This allows any Cloud resource provider that is interested in integrating with the EGI Cloud Infrastructure Platform to either deploy one of the Cloud Management Framework that have already been integrated, or to undertake the work necessary to integrate their existing deployment into the testbed.

The main accomplishments in PY4 are:

- The integration of cloud services into the operations infrastructure already running in production for the High Throughput Data Analysis Platform;
- The collection of many use cases and the running of Proof of Concepts demonstrating the applicability of the EGI Federated Coud IaaS services to address multiple user requirements, and defining the future technical roadmap;
- The launch of the production activities of the EGI Federated Cloud Solution during PQ17 at the EGI Community Forum 2014;

- The demonstration of the interoperability of the EGI Federated Cloud with cloud commercial providers and the participation of EGI to the Helix Nebula Marketplace[1] that was launched in May 2014.

[1] http://hnx.helix-nebula.eu/

[2] http://www.sienainitiative.eu

TABLE OF CONTENTS

1 INTRODUCTION

EGI has strategically decided to investigate how it could broaden the support to multiple research communities and application design models by enriching the solutions being offered with the aim of being able to take advantage of the existing functionality and investment already made in EGI's Core Infrastructure, but also support different research communities and their applications on the current production infrastructure than it was previously able to.

The utilisation of virtualization and Infrastructure as a Service (IaaS) cloud computing is a clear candidate to enable this transformation. It was also clear that with a number of different open source technologies already in use across a number of different resource providers, that it would not be possible to mandate a single software stack. Instead, following on from a number of different activities already on-going in Europe including SIENA[2], an approach that required the utilisation of open standards where available and, where not, methods that have broad acceptance in the e-infrastructure community were essential.

The Task Force as originally configured had an 18-month mandate starting from September 2011, which was subdivided into 3 succinct six-month blocks:

1) **Setup** – Identify resource and technology providers and draft the model,
2) **Consolidation** – Engage exemplar user communities and start configuration of test-bed,
3) **Integration** – Evolve the test-bed into a federated production IaaS infrastructure.

Overall goals for the activity are to:

- Write a blueprint document[3] for EGI Resource Providers that wish to securely federate[4] and share their virtualised environments as part of the EGI production infrastructure;
- Deploy a test bed[5] to evaluate the integration of virtualised resources within the existing EGI production infrastructure for monitoring[6], accounting[7] and information services[8];
- Investigate and catalogue the requirements[9] for community facing services based on or deployed through virtualised resources;
- Provide feedback[10] to relevant technology providers on their implementations and any changes needed for deployment into the production infrastructure;
- Identify and work with user communities[11] willing to be early adopters of the test bed infrastructure to help prioritise its future development;
- Identify issues[12] that need to be addressed by other areas of EGI (e.g. policy, operations, support & dissemination),
- Evolve the testbed into a production infrastructure.

[2] http://www.sienainitiative.eu
[3] https://wiki.egi.eu/wiki/Fedcloud-tf:Blueprint
[4] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:_Federated_AAI
[5] https://wiki.egi.eu/wiki/Fedcloud-tf:Testbed
[6] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Scenario5
[7] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Scenario4
[8] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Scenario3
[9] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:_Outreach#Requirements
[10] https://wiki.egi.eu/wiki/Fedcloud-tf:Blueprint:Solutions_Intentory
[11] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:_Outreach
[12] https://wiki.egi.eu/wiki/Fedcloud-tf:Blueprint:Security_and_Policy

This document represents a distilled version of the blueprint as it exists in the EGI Wiki as a collaborative source version. The test-bed is available since the early days of the Task Force, which then in turn was used to deploy a variety of Virtual Machines coming from diverse User Communities according to their requirements. Collaborating Technology Providers responded to requests for change in their respective software, and are continuing to do so: For example, new probes were developed that are planned to be integrated into EGI's Monitoring framework, and some changes to the EGI Accounting infrastructure were necessary to accommodate Cloud accounting requirements. A number of issues were found that required at the very least attention of some of EGI's policy groups. For example, the question of certifying Cloud Resource Providers for integration into the EGI production infrastructure raised a number of issues related to operational security that need to be addressed.

During PY3 and PY4, the EGI Federated Clouds Task Force was transformed into a funded task within the EGI-InSPIRE project, and the Task Force's mandate was integrated into the project's DoW as description of Task TSA2.6, being extended with the goal to transition the Task's test bed (or a part) into EGI's production infrastructure. As such the format of naming 6 monthly sprints was continued.

4) PreProduction – Scope the requirements for both resource providers and core services to reach production.
5) Prep4Production – Trial the processes by which resource providers can become certified members of the EGI e-infrastructure. Integrate new cloud specific core services into the

The task remains inclusive in terms of collaboration; some members are partially funded through EGI-InSPIRE and work together with unfunded members of the project, as well as members from outside the EGI-InSPIRE project.

The final phase ended officially in May 2014 with the announcement during the EGI Community Forum 2014 of the move to production status[13].

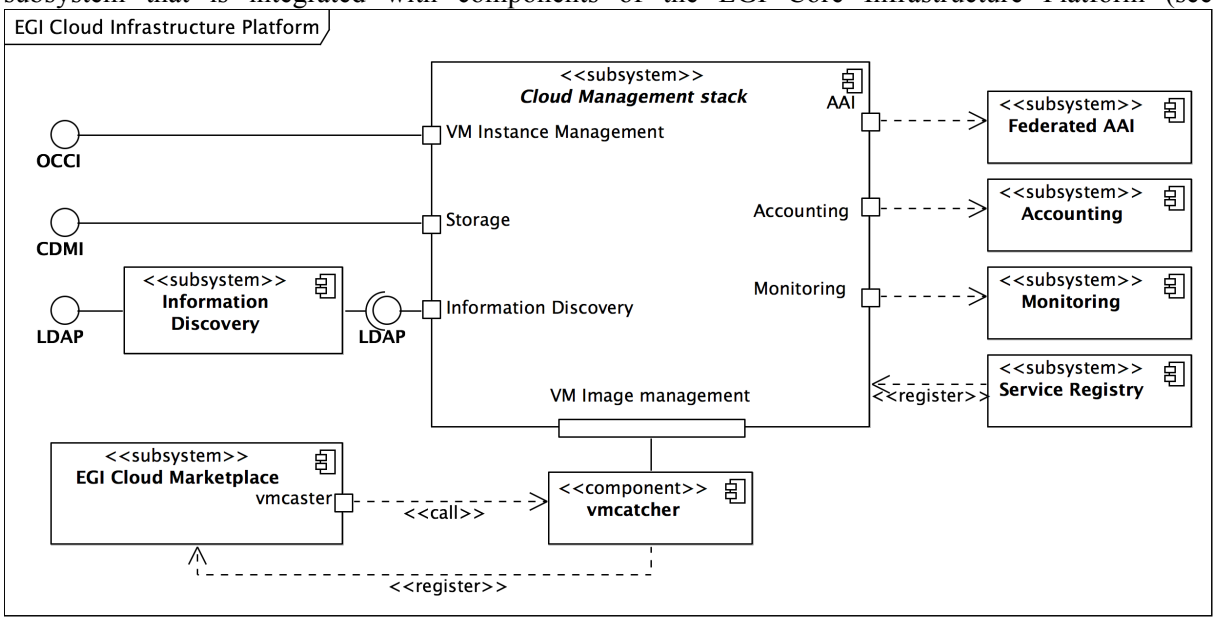
[13] http://www.egi.eu/news-and-media/newsfeed/news_2014_023.html

2 FEDERATION MODEL

The federation of IaaS Cloud resources in EGI is built upon the extensive autonomy of Resource Providers in terms of ownership of and hence user authorisation for access to exposed resources. The federation model for distributed IaaS Cloud resources allows a lightweight aggregation of local Cloud resources into the EGI CLoud Infrastructure Platform (CLIP). At the heart of the federation are the locally deployed Cloud Management stacks.

In compliance with the Cloud computing model, the EGI CLIP does not mandate deploying any particular or specific Cloud Management stack; it is the responsibility of the Resource Providers to investigate, identify and deploy the solution that fits best their individual needs whilst ensuring that the offered services implement the required interfaces and domain languages. These interfaces and domain languages, and the interoperability of their implementation with other solutions are the focus of the federation.

Consequently, the EGI CLIP is modelled around the concept of an *abstract* Cloud Management stack subsystem that is integrated with components of the EGI Core Infrastructure Platform (see Figure 1).



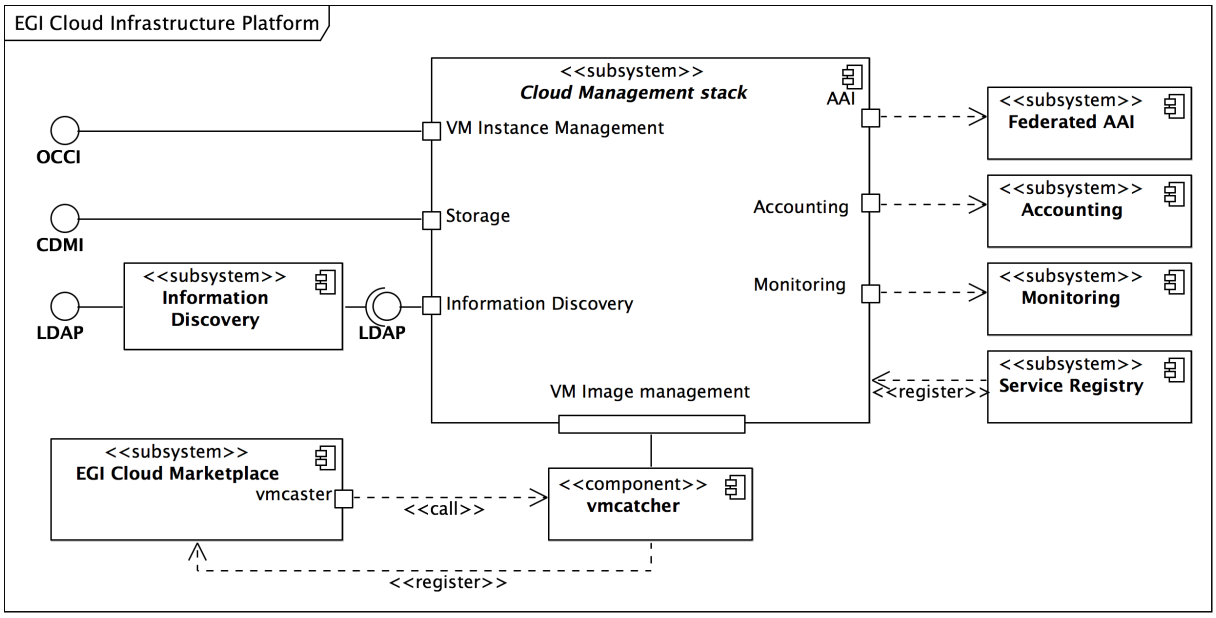


Figure 1: Architecture of the EGI Cloud Infrastructure Platform

This architecture allows EGI to define the CLIP as a relatively thin layer of federation and interoperability services around local deployments and integrations of Cloud Management stacks.

This architecture defines interaction ports with a number of services from the EGI Core Infrastructure Platform, and the EGI Collaboration Platform. At the same time, it defines the required external interfaces and corresponding interaction ports. All these ports will have to be realised by local Cloud Management stack deployments.

The main interaction points of Resource Providers depending on the local requirements, and include:

- The integration with the EGI Core Authentication & Authorisation Infrastructure
- The integration with the EGI Core Accounting system
- The integration with the EGI Core Monitoring system
- The provisioning of a standardised Cloud Computing management interface (OCCI)
- The provisioning of a standardised Cloud Storage interface (CDMI)
- The provisioning of a standardised interface to an Information Service.

Additionally, by means of using the Appliance Repository and the VM Marketplace from the EGI Collaboration Platform the EGI Cloud Infrastructure Platform is providing VM image sharing and re-use across EGI Research Communities.

Figure 2 provides an overview of the current realisations of the abstract Cloud Management stack subsystem in the EGI Cloud federation. It illustrates that each existing realisation inherits the obligation to implement the interaction points from the generalised parent Cloud Management stack. At the same time, the EGI Federated Clouds Task (funded through the EGI-InSPIRE project) gives Resource Providers a platform to share their implementation solutions for a commonly deployed specific Cloud Management stack (e.g. OpenNebula and OpenStack). Section 5 is dedicated to the documentation of the steps necessary to integrate a local deployment of a given Cloud Management stack into the EGI Cloud federation.

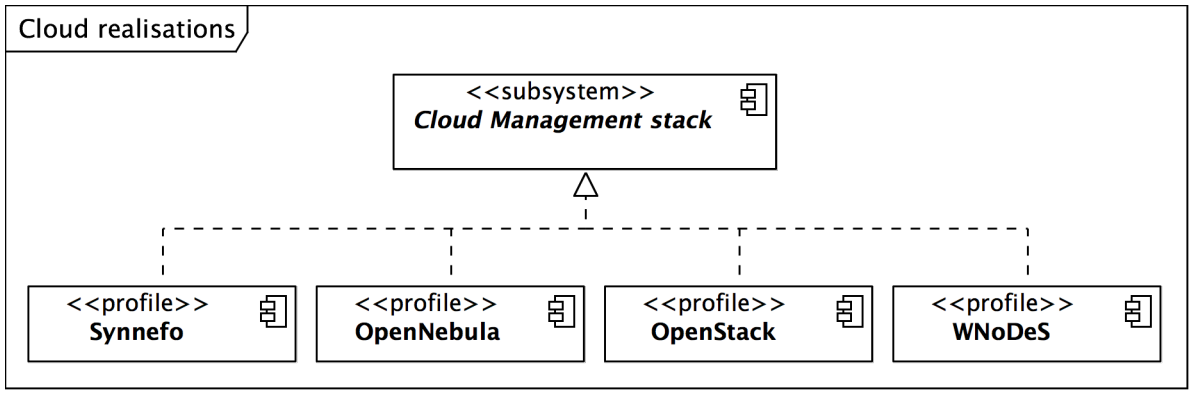


Figure 2: Current realisations of the abstract Cloud Management stack component

Through this collaboration, Resource Providers gradually develop and mature deployment and configuration profiles around common Cloud Management stacks as illustrated in Figure 2.

Through mutual support Resource Providers begin to build communities around the deployed Cloud Management Frameworks – the result is better integration of the most popular Cloud Management Frameworks in the Federated Clouds Task as illustrated in Table 1 below.

Cloud Mgmt. Stack	Integration					
	Fed. AAI	Monitoring[14]	Accounting	Img. Mgmt.	OCCI	CDMI
OpenStack	Yes	Yes	Yes	Yes	Yes	Yes
OpenNebula	Yes	Yes	Yes	Yes	Yes	Yes
Synnefo	Yes	Yes	-	-	Yes	Yes
WNoDeS*	Yes	-	-	-	Yes	-

Table 1: Overview of available integration for deployed Cloud Management Frameworks *The WNoDeS software is being deprecated though is still available without any sites currently running it.

2.1 Overview of requirements scenarios

The initial plan for federation of cloud resources within EGI was based on 6 different functional requirements that a user or community may have with regard to cloud technologies. Though dealt with separately we envisaged that the scenarios in some cases would build upon each other. These scenarios have expanded in number since original formation to include 4 further scenarios.

2.1.1 Scenario 1: VM Management

> "I want to start a single existing VM image on a remote cloud."

This scenario describes the details of managing the operation of a specific single VM image. It intentionally ignores any other cloud type functionality including data and information management.

[14] Monitoring is a passive activity, i.e. no active integration from the side of Cloud Management Frameworks is necessary.

The key aspect here is the use of virtualization to separate consumer from provider with the focus of this scenario lying on VM management operations.

2.1.2 Scenario 2: Managing my own data

This scenario extends scenario 1 by adding the following statements:

```
"I want to start a VM instance from an image that I have created."
"I want to associate my running VM with a data set in the Cloud."
"I want to take snapshots of my running VM for restart purposes"
```

This scenario extends the usage of a federated Cloud deployment by mixing in the capability to configure remote or (Cloud provider-) local data storage for use while the VM is executing.

Additional use cases that fall under the same scenario are:

- Using custom VM images created/administered by someone external to the Cloud provider:
  - If not provided by other means, some VM image upload/download facilities are required;
  - Storage facilities for VM images;
- Support for local, and remote storage locations to be configured for the VM.
- Taking a snapshot of a running VM

2.1.3 Scenario 3: Integrating multiple resource providers

This scenario includes scenario 2, plus the following statements:

```
"I want to choose on which resource provider I want to start my
single VM."
"I need to know about the VMM capabilities the provider offers."
```

This is the first scenario where the concept of multiple different cloud providers is introduced. The statements indicate that a user (or user group) must be able to decide with which resource provider (or a group) he or she would want to engage in business with. To allow this the scenario deals with information publication and dissemination across resource providers as follows:

- Information must be conveyed in a comparable manner (preferably through an open standard)
- Information must be publicly available
- Information must be human-readable, as well as accessible for automated queries (i.e. through an API)

2.1.4 Scenario 4: Accounting across Resource Providers

This scenario includes scenario 3, plus the following statements:

```
"My usage across different resource providers needs to be recorded
and reported to multiple aggregators."
```

This scenario deals with how to account for resource usage. Building on the well-understood accounting of resource currently within EGI addition questions within the scenario are;

- What actually are resources that may be consumed, and thus be accounted for? (Not to forget billing for commercial providers!)
- Once identified, what is the accounting unit for such resources?
- What is the metering interval/frequency? Is this identical across providers, or must this be provided as part of the information available in Scenario 3?

- At which level of detail should be accounting data collected?
- Where should the accounting data be stored? And who shall have access to it (on which detail?)

2.1.5 Scenario 5: Reliability/Availability of Resource Providers

To build a production infrastructure users must have confidence in the availability of resource sufficient to operate their tasks. This scenario includes scenario 4, plus the following statements:

> "Information relating to the reliability/availability and current status of the remote virtualised resource needs to be available to me."

This scenario deals with information about Resource Provider availability, which may influence a user's choice in selecting Resource Providers to engage with for further business. Also, a hypothetical Cloud federation may also put certain constraints on its members in terms of minimum availability and reliability in order to remain member of the federation. The following questions and issues need resolution:

- What are the exact semantics for availability and reliability?
- Which services are under monitoring for availability?
- How and where is this information collected and published?

2.1.6 Scenario 6: VM/Resource state change notification

> "When the status of the [VM] instance I am running changes (or will change) I want to be told about it."

This scenario supports the concept that any change in state of a resource or instance that a user or community are using should result in them being told about it.

- Reactive feedback about events in the past must be given.
- Proactive notification of *planned* changes must be provided, too.
- What is the format of notification?
- What are machine-readable requirements for notification to facilitate automation and user-managed reliability?

2.1.7 Scenario 7: AA across Resource Providers

> "I want to use my existing identity, and not re-apply for new credentials to use the service."

In common with many other activities across the research space the federated cloud should make use of federated identity. This will normally allow for a person to assert their identity based upon their employer when within the academic space or some other trusted identity provider. This may utilise online or token based technology and as such we would not desire to build our own but rather adopt a well-supported technology from elsewhere when available.

2.1.8 Scenario 8: VM images across Resource Providers

> "I want to use a single VM image across multiple different infrastructure providers"

This scenario deals with the requirement that the management of a user's VMs should be as simple as possible and when they have created an instance that they may wish to deploy widely across multiple providers then this should occur from a single catalogue. This scenario deals with the following issues:

- Provide a mechanism so that a user can upload transparently his own image to the test bed, with a unique global ID.
- Provide a common place to add an endorsement to a pertinent VM so that the resource providers can trust it.

2.1.9 Scenario 9: Brokering

> "I want my VM instance to run on a resource that is suitable based on a set of policies or requirements rather than my choosing directly which resource will run it"

A user must be able to easily and quickly decide which resource they wish to use and as such there must be a cloud brokering service. The goal is for a user to have a choice between a unified, abstracted view of the cloud test bed as a whole and the opportunity to target specific providers for their needs. As a consequence, this scenario is concerned with both brokers and management interface clients.

2.1.10 Scenario 10: Contextualisation

> "When I deploy a VM instance on a resource I must be able to give it configuration information for customisation of the default template. This can only happen when it is up and running"

Users must be able to configure automatically VM instances once they have been deployed on resources. Since they may be deployed on multiple resource providers this must take place automatically. There are a number of different possibilities for this type of configuration that the scenario explores. This will also allow resource providers to add any specific requirements on configuration they give on user communities.

3 HELIX NEBULA COLLABORATION

The EGI Federated Cloud has achieved a number of successful collaborations with the Helix Nebula initiative, all aimed to promote the interoperability between the commercial providers of the Helix Nebula initiative and the academic organizations members of the EGI Federated Cloud.

The result of these collaborations will ultimately make possible the exchange of workload between the EGI Federated Cloud and the HN providers, with the possibility to offload computational activities from public organizations resources offering institutional cloud services, where research and development are focused, to external commercial resources, where the commercial exploitation of the data is performed.

Within this scope, the technical interoperability work performed by EGI and SixSq enabled the first Helix nebula Blue Box release (based on SixSq's SlipStream software) to instantiate machines on the EGI Federated Cloud, making this a first example of interoperability between private and academic cloud services.

Furthermore, a copy of the Open Source SlipStream software was deployed into the EGI Federated Cloud and used to orchestrate part of the ESA Helix Nebula flagship application, demonstrating the possibility for the EGI Federated Cloud users to take advantage of the dynamic deployment and orchestration features of SlipStream.

With the migration of the Helix Nebula cloud to a production environment and the launch of the Helix Nebula Marketplace (HNX)[15], always based on the SlipStream technology, the EGI Federated Cloud participated actively to the building of such a marketplace, by both migrating and extending the support to the OCCI Federated Cloud standard interface to the new version of SlipStream in use into HNX. Also, in the topic of sustainability, some of the EGI Federated Cloud members proposed themselves as possible members of the HNX marketplace, being willing to sell, in fair competition and according to the national policies and regulations, part of their exceeding processing power directly to the scientists and other commercial customers via HNX.

The test of the new HNX marketplace technology within the EGI Federated Cloud is currently ongoing via the deployment of the CERN HN Flagship application into the EGI Federated Cloud via the HNX interface.

Last but not least, EGI will keep working closely with SixSq to provide the Federated Cloud standard interface for VM management, OCCI, as one of the northbound APIs available into SlipStream, and thus Helix Nebula HNX, future releases. This will ensure all the PaaS and SaaS technologies developed in the EGI Federated Cloud to work seamlessly into the commercial providers of Helix Nebula.

[15] http://hnx.helix-nebula.eu/

4 CLOUD SPECIFIC INTERFACES

To federate a cloud system there are several functions for which a common interface must be defined. These are each described below and overall provide the definition of the method by which a 'user' of the service would be able to interact.

4.1 VM management interface: OCCI

The Open Cloud Computing Interface (OCCI) is a RESTful Protocol and API designed to facilitate interoperable access to, and query of, cloud-based resources across multiple resource providers and heterogeneous environments. The formal specification is maintained and actively worked on by OGF's OCCI-WG, for details see http://occi-wg.org/. The intended deployment is depicted in Figure 3.

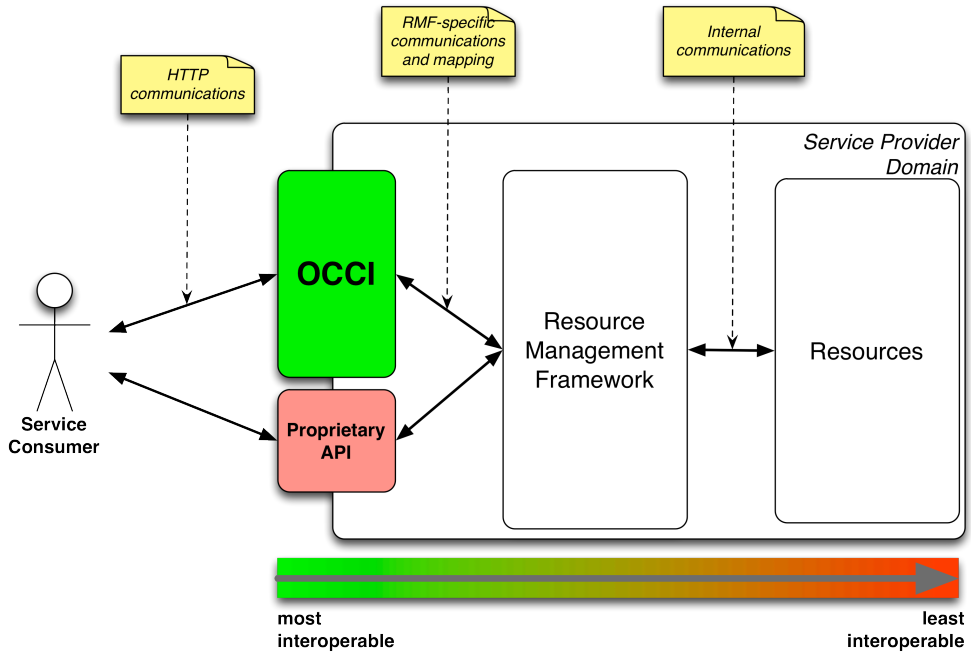


Figure 3: Deployment of OCCI in a provider's infrastructure

OCCI's specification consists of three basic elements, each covered in a separate specification document:

OCCI Core describes the formal definition of the OCCI Core Model [R 1]. **OCCI HTTP Rendering** defines how to interact with the OCCI Core Model using the RESTful OCCI API [R 2]. The document defines how the OCCI Core Model can be communicated and thus serialised using the HTTP protocol. **OCCI Infrastructure** contains the definition of the OCCI Infrastructure extension for the IaaS domain [R 3]. The document defines additional resource types, their attributes and the actions that can be taken on each resource type. Detailed description of the abovementioned elements of the specification is outside the scope of this document. A simplified description is as follows.

OCCI Core defines base types **Resource**, **Link**, **Action** and **Mixin**. Resource represents all OCCI objects that can be manipulated and used in any conceivable way. In general, it represents provider's resources such as images (Storage Resource), networks (Network Resource), virtual machines (Compute Resource) or available services. Link represents a base association between two Resource

instances; it indicates a generic connection between a *source* and a *target*. The most common real-world examples are Network Interface and Storage Link connecting Storage and Network Resource to a Compute Resource. Action defines an operation that may be invoked, tied to a specific Resource instance or a collection of Resource instances. In general, Action is designed to perform complex high-level operations changing the state of the chosen Resource such as virtual machine reboot or migration. The concept of mixins is used to facilitate extensibility and provide a way to define provider-specific features.

In the Federated Cloud environment, OCCI is deployed as a variety of platform-specific implementations. An ongoing EGI-InSPIRE mini-project[16] aims to provide a common implementation to further improve interoperability.

4.2 Data management interface: CDMI

The SNIA Cloud Data Management Interface (CDMI) defines a RESTful open standard for operations on storage objects [R 4]. Semantically the interface is very close to AWS S3 and MS Azure Blob, but is more open and flexible for implementation.

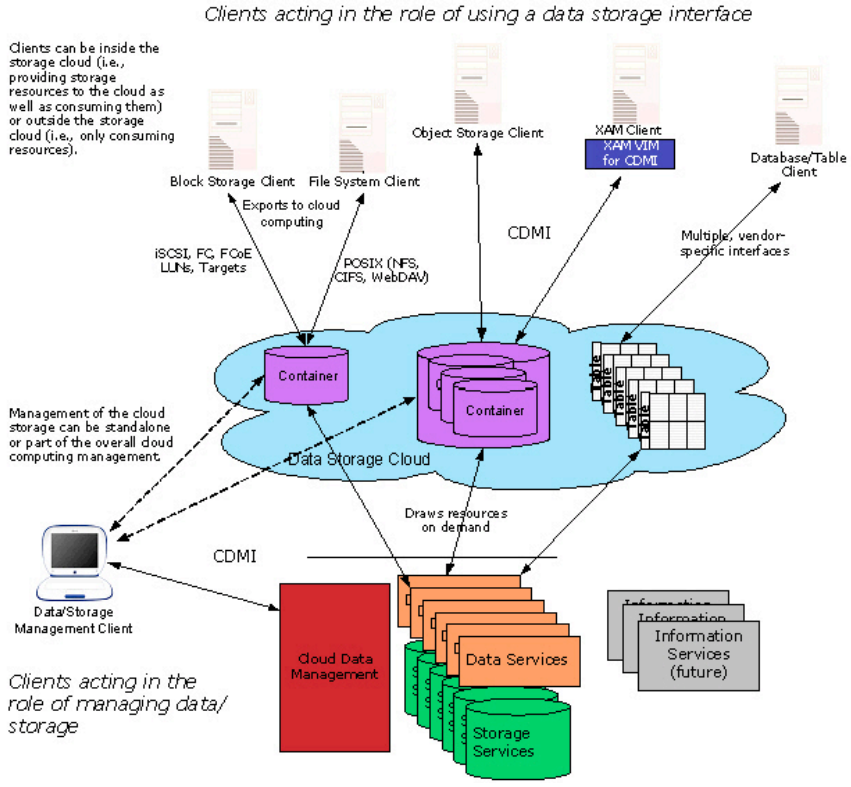


Figure 4: Cloud storage reference model (courtesy to SNIAcloud.com)

Figure 4 shows the conceptual model of a cloud storage system. CDMI offers clients a way for operating both on a storage management system and single data items. The exact level of support depends on the concrete implementation and is exposed to the client as part of the protocol.

The design of the protocol is aimed both at flexibility and efficiency. Certain heavyweight operations, e.g. blob download, can be performed also with a pure HTTP client to make use of the existing

[16] TSA4.4 Providing OCCI support for arbitrary Cloud Management Frameworks

ecosystem of tools. CDMI is built around the concept of Objects, which vary in supported operations and metadata schema. Each Object has an ID, which is unique across all CDMI deployments.

4.2.1 CDMI Objects

There are 4 objects most relevant in the context of EGI's Federated Cloud:

- **Data object**: Abstraction for a file with rich metadata.
- **Container: A**bstraction for a folder. Export to non-HTTP protocols is performed on the container level. Container might have other containers inside of them.
- **Capability:** Exposes information about a feature set of a certain object.
- **Domain:** Deployment specific information.

4.2.2 Detection of capabilities

CDMI supports partial implementation of the standards by defining optional features and parameters. In order to discover what functionality is supported by a specific implementation, CDMI client can issue a GET request to a fixed url: /cdmi_capabilities.

More information about the CDMI standard can be found at http://cdmi.sniacloud.com/.

4.2.3 CDMI extensions for FedCloud

For the Federated Cloud environment, the primary goal of CDMI is to offer a standard interface for operating with blob data. The interface can be offered either through a native interface of the cloud stack, or through a CDMI proxy developed in FedCloud. The proxy includes authentication and authorization extensions for connecting to OpenStack Keystone and through that to FedCloud/EGI trust system.

4.3 Virtual Organisation Management & AAI: VOMS

Within EGI, research communities are generally identified and, for the purpose of using EGI resources, managed through "Virtual Organisations" (VOs). Naturally, support for VOs is also compulsory for the EGI Cloud Infrastructure Platform. For the purpose of the Federated Cloudstask, a single VO "fedcloud.egi.eu" is used to provide access to the task's testbed. Additionally, for monitoring purposes, Cloud Resource Providers are required to provide access to the "ops" VO to properly integrate with the EGI Core Infrastructure Platform.

Integration modules are available for each Cloud Management Framework that been developed by the task members. Configuring these modules into a provider's cloud installation will allow members of these VOs to access the cloud. Figure 5 shows the main components involved. The user retrieves a VOMS attribute certificate from the VOMS server of the desired VO (currently, Perun server for "fedcloud.egi.eu" VO) and thus creates a local VOMS proxy certificate. The VOMS proxy certificate is use in subsequent calls to the OCCI endpoints of OpenNebula or OpenStack using the rOCCI client tool. The rOCCI client directly talks to OpenNebula endpoints, which map the certificate and VO information to local users. Local users need to have been created in advance, which is triggered by regular synchronizations of the OpenNebula installation with Perun.

In order to access an OpenStack OCCI endpoint, the rOCCI client needs to retrieve a Keystone token from OpenStack Keystone first. The retrieval is transparent to the user and automated in the workflow of accessing the OpenStack OCCI endpoint. It is triggered by the OCCI endpoint rejecting invalid requests and sending back an HTTP header referencing the Keystone URL for authentication. Users are generated on the fly in Keystone, it does not need regular synchronization with the VO Management server Perun (see below).

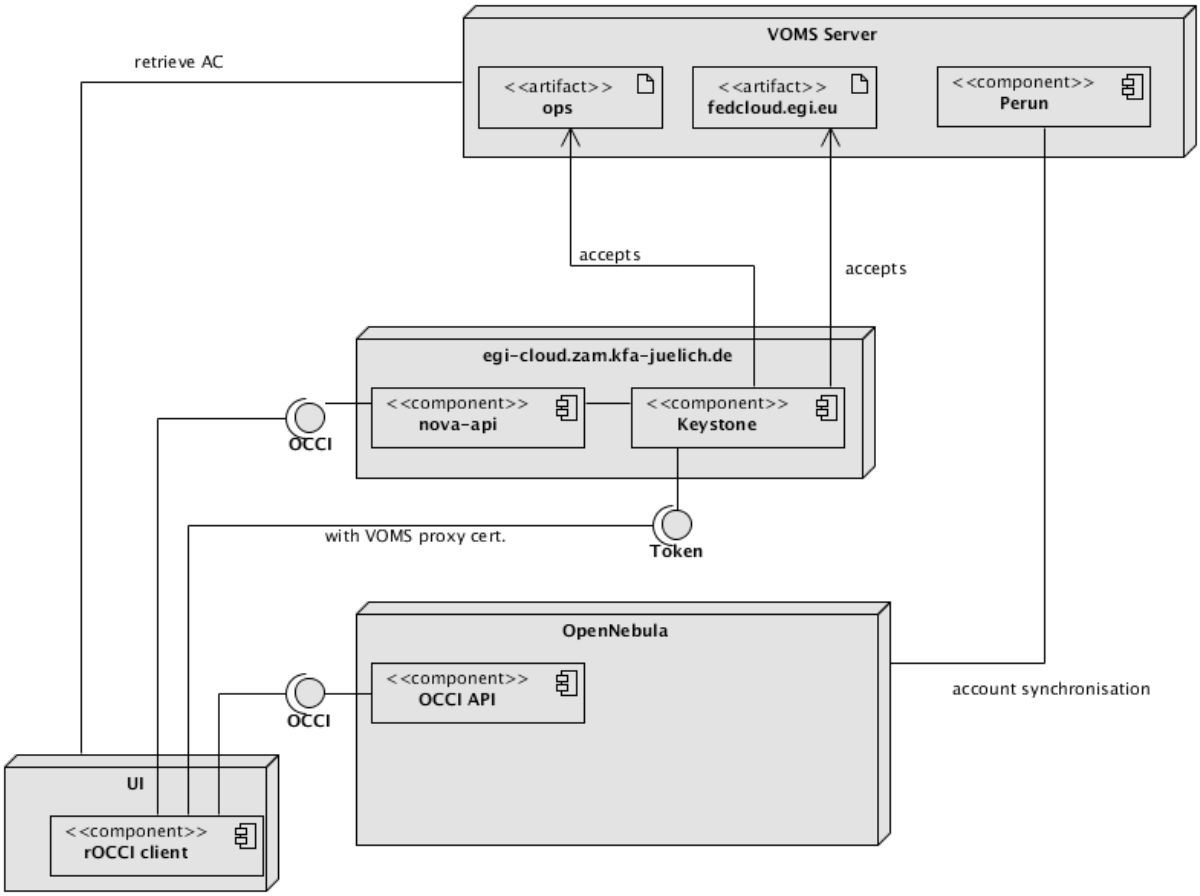


Figure 5: Model of the Federated Cloud authentication architecture

Generic information about how to configure VOMS support for;

- OpenStack Keystone can be found at http://keystone-voms.readthedocs.org/en/latest/. Information specific to FCTF is located at https://wiki.egi.eu/wiki/Federated_AAI_Configuration#OpenStack.
- OpenNebula, the information can be found here: https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:_Federated_AAI:OpenNebula.
- Stratuslab provides multiple authentication mechanisms at once. They are documented here: http://stratuslab.eu//documentation/2012/10/07/docs-syadmin-auth.html.

Since all of these different technology providers have developed their own systems then the functionality provided by the different services and methodology by which they use VOMS credentials etc., are slightly different.

4.4 VM Image management

In a distributed, federated Cloud infrastructure, users will often face the situation of efficiently managing and distributing their VM Images across multiple and heterogeneous Cloud resource providers. The VM Image management subsystem provides the user with an interface into the EGI Cloud Infrastructure Platform to notify supporting resource providers of the existence of a new or updated VM Image. Sites then examine the provided information, and pending their decision pool the new or updated VM Image locally for instantiation.

This concept introduces a number of capabilities into the EGI Cloud Infrastructure Platform:

- **VM Image lifecycle management** – Apply best practices of Software Lifecycle Management at scale across EGI
- **Automated VM Image distribution** – Publish VM images (or updates/removals of them), and their automatic distribution to the Cloud resource providers that support the publishing research community (Virtual Organizations in our case) with Cloud resources.
- **Asynchronous distribution mechanism** – Publishing images and pooling these locally are intrinsically decoupled, allowing federated Resource Providers to apply local, specific processes transparently before VM images are available for local instantiation.
- **Virtual Organization-specific VM image endorsement policies** – Not all federated Cloud resource providers will be able to enforce strict perimeter protection in their Cloud infrastructure as risk management to contain potential security incidents related to VM images and instances. Hence, each VO will be responsible to inspect and endorse a group of VM Images and make them available for being pooled by the sites. On the other hand, its up to the sites to implement an additional VM Image specific inspection and assessment policy prior to pooling the image for immediate instantiation.

One service, the EGI Applications Database and two command-line tools, the “vmcaster” and the “vmcatcher” provide the principal functionality of this subsystem.

The EGI Applications Database is the VM Image marketplace, with main role to hold and populate Images related metadata as provided by the user communities, and to provide the necessary mechanism for automatic distribution of the Images (endorsed or not) to the sites.

"Vmcatcher" is the command line tool responsible for subscribe to the lists produced by the EGI Applications Database, and finally, "vmcaster" is capable of publishing, ready to be used image lists, either directly to the EGI Applications Database or to any other 3rd-party web server.

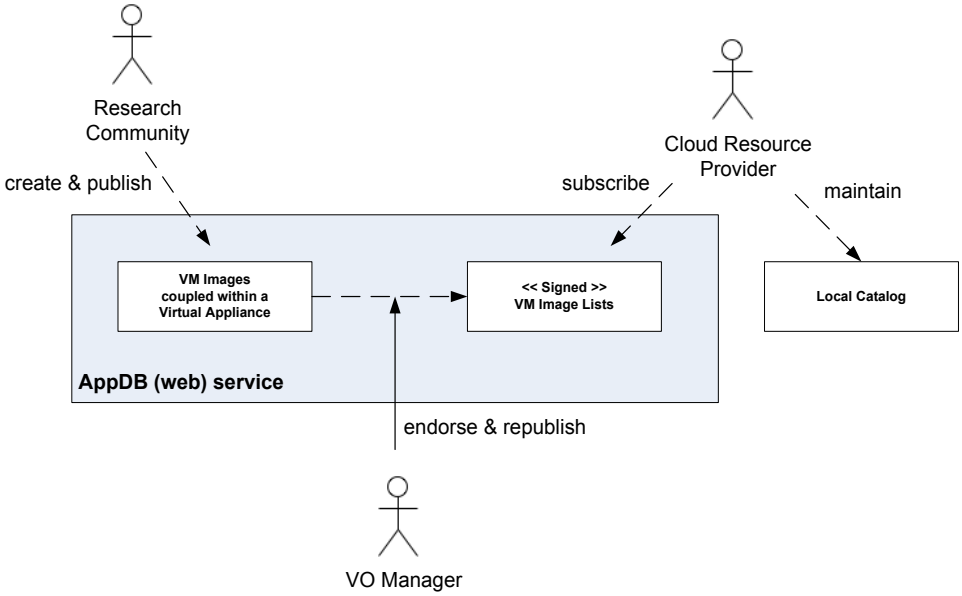


Figure 6: Main components and actors of the VM Image management subsystem

Research Communities ultimately create and update VM Images (or delegate this functionality). The Images metadata are stored in the EGI Applications Database and the Images themselves are stored in distributed appliance repositories that are provided and managed elsewhere, typically by the Research Community itself.

Through the EGI Applications Database service, an authorized representative of the Research Community (so called 'VO Manager'), composes a VM Image list (or updates an existing one) with Images that are considered as of interest by his community and then (re-)publishes it.

Federated Clouds Resource Provider then subscribe to changes in VM Image lists by regularly downloading the list from the EGI Applications Database, and comparing it against local copies. New and updated VM Images are downloaded from the appliance repository referenced in the VM Image list into a local staging cache and, where required, made available for further examination and assessment.

Ultimately, Cloud resource Providers will make VM Images available for immediate instantiation by the Research Community.

4.4.1 Image Contextualisation

Contextualization is the process of installing, configuring and preparing software upon boot time on a pre-defined virtual machine image (e.g. setting the hostname, IP addresses, SSH authorized keys, starting services, installing applications, etc.). We have identified as a requirement to contextualize images the possibility of passing user provided data to the VM when they are instantiated. Hence there were two things to be defined:

- How to pass data upon VM creation (the exact type and format of the data should not be relevant, it should be up to the user),
- How to retrieve those data from the running VM.

For passing the data we have proposed the use of a new OCCI mixin that has an attribute to hold the data to pass to the image. The second part, related to retrieving the data, is more dependent of the back-end implementation. There are different methods in the systems in place in FedCloud, but the selected tool cloud-init handles these possible differences in a transparent way for the users.

4.4.1.1 Cloud-init

This task force recommends the use of cloud-init for the contextualization of VMs. Cloud-init frees the user from managing the specific ways for handling the contextualization information and it's widely available in most OS versions and IaaS cloud platforms. The latest versions support OpenNebula contextualization mechanisms. OpenStack and Synnefo contextualization are supported in most cloud-init versions (datasources are EC2 and NoCloud). By default cloud-init will:

- Put the ssh-key into the `~/.ssh/authorized_keys` of root user (or equivalent)
- If the user provided data is a script, it will be executed upon instantiation.

More complex use-cases are supported, with documented examples in regular cloud-init documentation.

5 EGI CORE SERVICES FOR CLOUD

Alongside implementations of cloud specific interfaces it is necessary to enable the connection of these new service types with the core EGI services of Accounting, Monitoring and Service Discovery.

5.1 Information discovery: BDII

Users and service managers need tools to retrieve information about the whole infrastructure and filter the returned data to select relevant subsets of the infrastructure that fulfil their requirements. To achieve this target the information about the services in the infrastructure must be structured in a uniform schema and published by a common set of services usable both by automatic tools and human users.

The current standard deployed in EGI for the implementation of the common information system is the Berkeley Database Information Index (BDII). This software is based on a LDAP server, deployed in a hierarchical structure and distributed over the whole infrastructure. The information system is structured in three levels: the services publish their information (e.g. specific capabilities, total and available capacity or user community supported by the service) using an OGF recommended standard format, GLUE2 [R6]. The information published by the services is collected by a Site-BDII, a service deployed in almost every site in EGI. The Site-BDIIs are queried by the Top-BDIIs - a national or regional located level of the hierarchy, which contain the information of all the site services available in the infrastructure and their services. NGIs usually provide an authoritative instance of Top-BDII, but every Top-BDII, if properly configured, should contain the same set of information.

Users and tools can use the Top-BDII to look for the services that provide the capabilities and the resources to run their activities. A typical example of Top-BDII query is retrieving the list of services that support a specific user community or VO.

At the time of the writing, the Cloud federation platform integrates the EGI Core Information discovery system. The Cloud resources are published under the same tree as the Grid ones, but grouped in a different sub-group at site level. This permits a site to publish Cloud and Grid services at the same time and for a user to query specifically for Cloud or Grid within the same infrastructure.

The current integration uses the GLUE2 schema to represent both Cloud and Grid resources. Even if the GLUE2 schema defines generic computing and storage entities, it was developed originally for Grid resources and can represent only partially the information needed by the Cloud users. Thus, the EGI Federated Cloud is working within the GLUE2 WG at OGF to profile and extend the schema to represent Cloud Computing, Storage and in the future Platform and Software services. The proposed extensions are currently under discussion at the WG.

Most of the data currently published is semi-static data, configured manually by the site administrator during installation and update of the infrastructure. To reduce the operational costs, the EGI Federated Cloud is currently working on a system to retrieve the semi-static data (eg. resources and OS templates provided) automatically from the Cloud Middleware and complement this data with dynamic information (e.g. currently running VMs and status of utilization of the services).

5.2 Central service registry: GOCDB

EGI's central service catalogue is used to catalogue the static information of the production infrastructure topology. The service is provided using the GOCDB tool that is developed and deployed within EGI. To allow Resource Providers to expose Cloud resources to the production infrastructure, following service types were added to GODCB:

- eu.egi.cloud.accounting
- eu.egi.cloud.broker.compss

- eu.egi.cloud.broker.proprietary.slipstream
- eu.egi.cloud.broker.vmdirac
- eu.egi.cloud.information.bdii
- eu.egi.cloud.storage-management.cdmi
- eu.egi.cloud.vm-management.occi
- eu.egi.cloud.vm-metadata.marketplace.

Initially registered Cloud resources were maintained in test-bed mode to protect the production infrastructure from side effects originating from the task's federated Clouds test-bed. In the process of Cloud resource certification sites and services endpoints were moved to production mode, thus enabling SAM to calculate availability and reliability for Cloud resources.

5.3 Monitoring: SAM

The SAM (Service Availability Monitoring) system is a framework consisting of:

- Nagios monitoring system (https://www.nagios.org),
- Custom databases for topology, probes description and storing results of tests
- web interface MyEGI (http://mon.egi.eu/myegi)

Probes to check functionality and availability of services must be provided by service developers. More information on SAM can be found at https://wiki.egi.eu/wiki/SAM. The current set of probes used for monitoring cloud resources consists of:

- OCCI probe: Creates an instance of a given image by using OCCI and checks its status
- BDII probe: Basic LDAP check tries to connects to cloud BDII
- Accounting probe: Checks if the cloud resource is publishing data to Accounting repository
- TCP checks: Basic TCP checks used for CDMI and broker services.

More information on cloud probes can be found here: https://wiki.egi.eu/wiki/Cloud_SAM_tests.

A central SAM instance specific to the activities of the EGI Federated Clouds Task has been deployed for monitoring test bed (https://cloudmon.egi.eu/nagios). Results of cloud probes are visible on the central SAM interface (http://mon.egi.eu/myegi) under profile ch.cern.sam-CLOUD-MON. The available probes are in flux and as such once finalized these will be included into official SAM release. Adding probes to official SAM will follow procedure "Adding new probes to SAM" (https://wiki.egi.eu/wiki/PROC07).

The Operations Portal combines and harmonizes different static and dynamic information and enables the operators to manage alarms coming from the SAM system. Operators use the dashboard to react on alarms, interact with sites, provide first-level support and perform oversight of alarms and manage tickets on national level. The procedure "Setting a Nagios test status to operations" (https://wiki.egi.eu/wiki/PROC07) defines how to add new test to a list tests which generate alarms in the Operations Portal. The following SAM tests were added to operations tests:

- eu.egi.cloud.OCCI-VM
- org.nagios.CloudBDII-Check
- org.nagios.OCCI-TCP.

Other tests run but not yet in the central SAM instance are;

- eu.egi.cloud.APEL-Pub
- org.nagios.Broker-TCP

- org.nagios.CDMI-TCP

Other tests in development include those that will verify the VMCaster operation and in the longer term the capability of the cloud itself with some form of benchmarking.

5.3.1 Operational Certification

Resource Center Certification is a verification process enabling a particular resource provider to become part of a Resource Infrastructure such as a National Grid Initiative (NGI), an EIRO, or a multi-country Resource Infrastructure. It describes steps involved to both register and certify new Resource Centers in the EGI Production infrastructure.

In order to facilitate certification of Resource Centers providing cloud resources, temporary Cloud Resource Center Registration and Certification procedure has been created [https://wiki.egi.eu/wiki/PROC18]. This was to detect steps in the existing procedure [https://wiki.egi.eu/wiki/PROC09] that do not apply, taking into account different nature of federated cloud platform and its maturity, and also to simplify in first phase of the integration. After testing phase both procedures will be merged.

The procedure is both a strict technical and operational personnel based procedure. It involves the nominations of responsible members of staff with their details recorded and then the quality of the technical infrastructure being assessed through the output of the monitoring infrastructure.

5.4 Accounting

To account for resource usage across the resource providers the following have been defined:

- The particular elements or values to be accounted for;
- Mechanisms for gathering and publishing accounting data to a central accounting repository;
- How accounting data will be displayed by the EGI Accounting Portal.

The EGI Federated Clouds Task Usage Record which inherits from the OGF Usage record [R5] defines the data elements, which resource providers should send to the central Cloud Accounting repository. Not all of the agreed elements are currently sent by the accounting clients. Those elements are marked with an X in the following table. Development work continues to implement all of the agreed elements. The usage record is as follows:

Key	Value	Description	Mandatory
VMUUID	String	Virtual Machine's Universally Unique IDentifier	Yes
SiteName	String	Sitename, e.g. GOCDB Sitename	Yes
MachineName	String	VM Id	
LocalUserId	String	Local username	
LocalGroupId	string	Local groupname	
GlobalUserName	string	User's X509 DN	
FQAN	string	User's VOMS attributes	Yes
Status	string	Completion status - started, completed, suspended	
StartTime	int	Must be set if Status = Started (epoch time)	
EndTime	int	Must be set if Status = completed (epoch time)	
SuspendDuration	int	Set when Status = suspended (seconds)	

Key	Value	Description	Mandatory
WallDuration	int	Wallclock - actual time used (seconds)	
CpuDuration	int	CPU time consumed (seconds)	
CpuCount	int	Number of CPUs allocated	
NetworkType	string	Description	Yes
NetworkInbound	int	GB received	Yes
NetworkOutbound	int	GB sent	Yes
Memory	int	Memory allocated to the VM (MB)	Yes
Disk	int	Disk allocated to the VM (GB)	Yes
StorageRecordId	string	Link to associated storage record	Yes
ImageId	string	Image ID	
CloudType	string	e.g. OpenNebula, Openstack	

Scripts have been provided for OpenNebula and Openstack implementations to retrieve the accounting data required in this format ready to be sent to the Cloud Accounting Repository. These scripts are available from:

- OpenNebula – https://github.com/EGI-FCTF/opennebula-cloudacc
- Openstack –
  - https://github.com/EGI-FCTF/osssm (older versions)
  - https://github.com/schwicke/ceilometer2ssm (Grizzly onwards)
- Syneffo – internal Syneffo component

The APEL SSM (Secure STOMP Messenger) package is provided by STFC for resource providers to send their messages to the central accounting repository. It is written in Python and uses the STOMP protocol, the messages contain cloud accounting records as defined above.
The OpenNebula and Openstack scripts produce the messages to be sent using the SSM package in the correct format.
The SSM package can be downloaded from http://apel.github.io/apel/
Detail about configuring SSM and publishing records may be found here:
https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Scenario4#Publishing_Records

SSM utilizes the network of EGI message brokers and is run on both the Cloud Accounting server at STFC and on a client at the Resource Provider site. The SSM running on the Cloud Accounting server receives any messages sent from the Resource Provider SSMs and they are stored in an “incoming” file system.
A Record loader package also runs on the Cloud Accounting server and checks the received messages and inserts the records contained in the message into the MySQL database.
A Cloud Accounting Summary Usage Record has also been defined and the Summaries created on a daily basis from all the accounting records received from the Resource Providers is sent to the EGI Accounting Portal. The EGI Accounting Portal also runs SSM to receive these summaries and the Record loader package to load them in a MySQL database storing the cloud accounting summaries.

The EGI Accounting Portal provides a web page displaying different views of the Cloud Accounting data received from the Resource Providers[17].

5.5 Image metadata publishing & repository

The task uses the EGI Applications Database service (AppDB for short) as the virtual appliance marketplace, for storing and publishing images related metadata, while the physical location of the images could be on either the EGI appliance repository[18] or any other appliance repository managed by a Research Community.

In general, the EGI AppDB[19] is a central service that stores and provides to the public, information about software solutions in the form of native software products and virtual appliances, the programmers and the scientists who are involved, and publications derived from the registered solutions. 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 Infrastructures without reinventing the wheel. This way, scientists can spend less or even no time developing or porting 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. The EGI Applications Database is open to every scientist, interested in publishing and therefore sharing, their software solutions.

One of the most significant features offered by the service is the 'Cloud/Virtual Appliances Marketplace'[20] section, to support the uptake of EGI's new production infrastructure, the Federated Cloud. The new marketplace section enables the sharing of Virtual Appliances — sets of Virtual Machine images that belong to a single scientific application setup. The shared appliances are deployed on the sites of the Federated Cloud through Virtual Organizations, and can then be instantiated on-demand by VO members, using the provided command line tools of the Federated Cloud, or one of the high level, graphical environments contributed by the NGIs.

Besides metadata registration about Virtual Appliances, the Marketplace offers the ability to manage each appliance's images by defining and publishing versioned sets thereof, categorized by operating system, platform architecture, virtualization technology, etc. This image information may be easily distributed to any infrastructure (including the Federated Cloud one) by creating vmcatcher compatible image lists, or VO-wide image lists directly from within the AppDB portal; the image lists specify which site or VO, respectively, offers the specific version of the VA, so that users make use of them.

The main capabilities offered by the EGI Application Database is as follows:

A user or an image holder (submitter) is able to:

- browse the metadata for suitable images
- download images for local use
- register his own virtual appliance
- add one or more images to his virtual appliance
- update the images associated to his virtual appliance
- publish the virtual appliance and therefore makes it available to the public for further usage

[17] http://accounting-devel.egi.eu/cloud.php
[18] https://appliance-repo.egi.eu
[19] https://appdb.egi.eu
[20] https://appdb.egi.eu/browse/cloud

- get all the necessary usage details for instantiating an image to a site where the image is available.

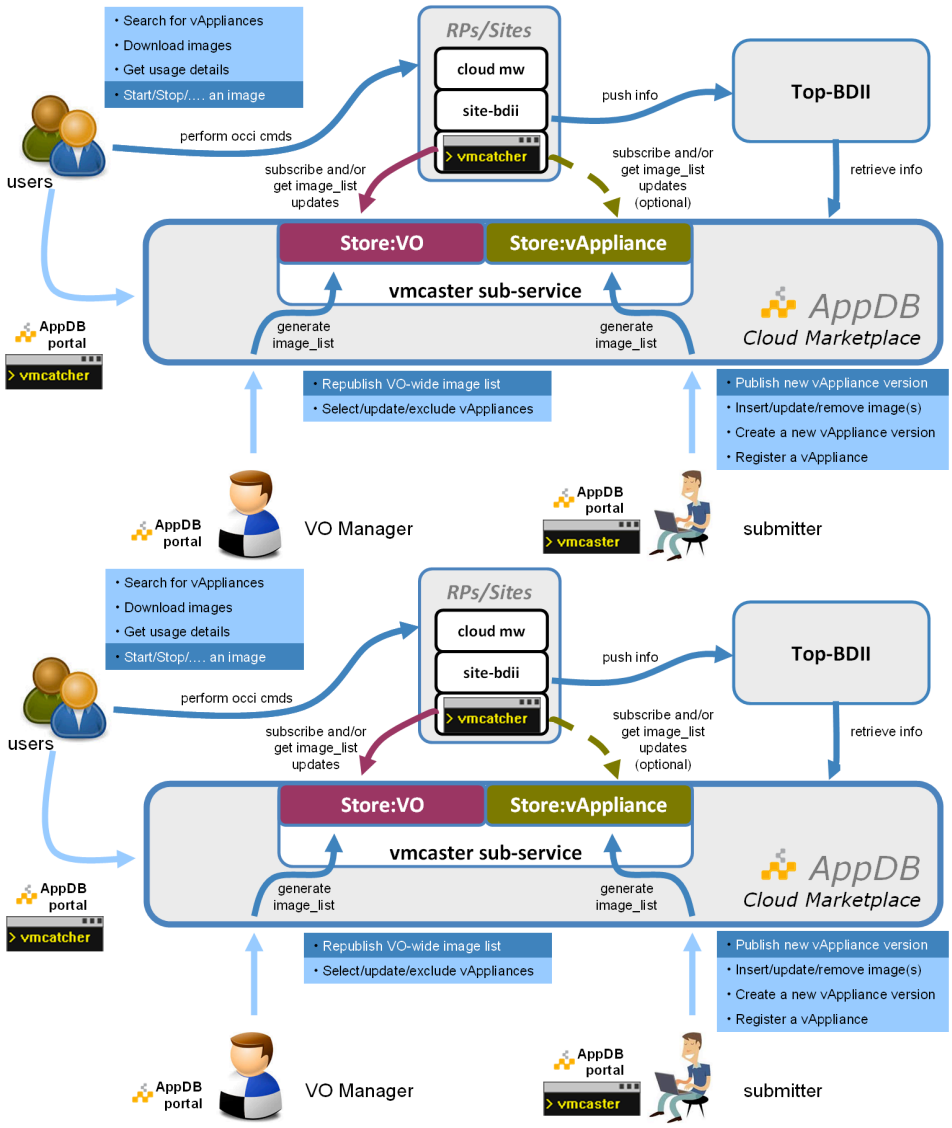


Figure 7: Using the EGI AppDB as Virtual Appliance Marketplace.

A VO manager (an authorized representative of a Research Community) is able to:

- select any of the register virtual appliances
- evaluate virtual appliance metadata and download the images for further inspection
- endorse the chosen images by publishing them into the VO-wide image list of his responsibility and therefore make them available for being pooled by the Resource Providers/Sites which supports the VO.

Finally, by using the vmcatcher tool, the site administrator:

- subscribes to the VO-wide image list as this composed by the VO manager

- fetches images metadata and image files (the files could be served by any appliance repository, including the EGI one)
- pushes the images & metadata to the Cloud middle-ware the site maintains
- updates the information system of the infrastructure

6 FEDERATING CLOUD RESOURCES TO EGI

The model of federation chosen in the EGI is one where all resources available to the user are equal. This is therefore suitable for resource consumers who do not have their own cloud infrastructure available to them. Within this section we detail the concepts behind the method of federation chosen and how those technology providers within the task force have been able to adapt or integrate their technologies. We therefore have for each technology provider a section which details work done for integration and any specific configuration a deployer of this technology needs to do to connect to EGI. We also describe the technology premise that the activity itself started with.

During the task force stage of the activity membership of the federated cloud activity was obtained through approach to the activity chair and attendance at the weekly group meeting. As we move towards a production infrastructure we must move beyond this to a moderated and measured basis by which resource providers are able to claim membership of the cloud. As such we aim to build upon the different procedures already in place as well as the standards by which different interfaces to resources are supported.

This will include a certification process[21] by which official membership of the cloud is allowed and through the dedication of resources to the activity. This will be measured through the monitoring process previously described and passing of tests, which will enable a certification of the resources a provider gives. We make no distinction as to the resource access model in terms of free at the point of use, charge at the point of use, bulk buy or other models of financial reconciliation.

In the following sections the underlying functions that the EGI Federated Cloud supports are described along with for each available technology the level of integration and any necessary changes from the default version of that technology.

6.1 OpenNebula

A new Resource Provider using OpenNebula or OpenNebula-based CMF has to take the following steps to technically join the EGI Cloud Federation. There is only one prerequisite and that is fully functional OpenNebula installation capable of deploying, sustaining and shutting down virtual machines. There are no requirements for the underlying architecture. Resource Providers in question may choose the virtualization platform, network and storage configuration according to their preferences and needs. It is highly recommended to install OpenNebula v3.8.x where x denotes the latest security update and coordinate any future upgrades with other Task members to avoid infrastructure fragmentation. Resource providers installing OpenNebula from scratch should follow its step-by-step installation and configuration guides available online[22].

The technical integration with the EGI Cloud Federation consists of the following steps:

1. Additional OpenNebula configuration
2. rOCCI-server installation and configuration
3. Integration with VO management service -- Perun
4. Integration with accounting service -- APEL
5. Integration with VM Image management service -- vmcaster/vmcatcher
6. Integration with information system -- LDAP/BDII
7. Registration of deployed services in GOCDB

[21] https://wiki.egi.eu/wiki/PROC09_Resource_Centre_Registration_and_Certification
[22] http://opennebula.org/documentation:archives:rel3.8

Each of the above-mentioned steps is a requirement for every Resource Provider wishing to join the EGI Cloud Federation. Resource Providers are welcome to deploy and offer additional services such as object storage (CDMI) but this is not a requirement at this time. Detailed description of the listed steps is as follows.

Additional OpenNebula configuration

Integration with EGI Cloud Federation requires the use of X.509 authentication mechanism in communication with OpenNebula. Resource Providers are encouraged to follow the step-by-step configuration guide provided by OpenNebula developers available online[23]. There is no need to change authentication driver for the *oneadmin* user or create any user accounts manually at this time.

rOCCI-server installation and configuration

The EGI Cloud Federation uses OCCI as its VM management protocol. It is necessary to install a fully compliant OCCI 1.1 server on top of RP's existing OpenNebula installation. OpenNebula's OCCI implementation is *not* compliant with the OCCI 1.1 specification. This functionality is provided by the rOCCI-server project. Detailed installation and configuration instructions are available online in the Task Wiki[24].

Integration with Perun

The current rOCCI-server implementation doesn't handle user management and identity propagation hence integration with a third-party service is necessary. The Perun VO management server developed and maintained by CESNET is used to provide user management capabilities for OpenNebula Resource Providers[25]. It uses locally installed scripts (fully under the control of the Resource Provider in question) to propagate changes in the user pool to all registered Resource Providers. They are required to install and configure (if need be) these scripts and report back to EGI Cloud Federation for registration in Perun. Installation and configuration details are available online in the Task's repository on GitHub[26].

Integration with APEL

One of the required integration points is accounting. The EGI Cloud Federation employs the APEL framework with extended accounting records. Every Resource Provider is required to install the APEL SSM client and OpenNebula accounting script. As with the previous cases, installation and configuration details are available online on GitHub and the Wiki[27].

Integration with VM Image Management infrastructure

Resource Providers are required to integrate their OpenNebula with an image management service used within the federation. As with the previous cases, installation and configuration details are available online in the wiki[28]. This service ensures that all images are trusted and up-to-date for all Resource Providers across the federation.

[23] http://opennebula.org/documentation:archives:rel3.8:x509_auth
[24] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:_Federated_AAI:OpenNebula
[25] http://perun.metacentrum.cz/web/
[26] https://github.com/EGI-FCTF/fctf-perun
[27] https://github.com/EGI-FCTF/opennebula-cloudacc
[28] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Scenario8:Configuration#VMcatcher

Integration with TopBDII

Details about services offered by the Resource Provider in question are advertised to the rest of the EGI Cloud Federation using an LDAP server -- BDII. Resource Providers are encouraged to follow instructions available online in the Wiki[29].

Registration in GOCDB

The procedure for registration of a resource provider within GOCDB is as per other types of resources within the EGI infrastructure[30].

6.2 OpenStack

This section describes steps necessary for new Resource Provider (RP) using Openstack middleware to join EGI Cloud Federation. It is strongly recommended using the last Openstack version. Specifically, the VOMS-enabled authentication will require Grizzly version of Keystone. The installation and configuration instructions for OpenStack are available online[31].

The actual integration with the EGI Cloud Federation consists of the following steps:

a) VOMS-enable Keystone installation and configuration
b) OCCI installation and configuration
c) Integration with accounting service APEL
d) Integration with VM Image Management infrastructure
e) Integration with information system
f) Registration of deployed services in GOCDB

Each of the above-mentioned steps is a requirement for every Resource Provider wishing to join the EGI Cloud Federation. Resource Providers are welcome to deploy and offer additional services such as object storage (CDMI) but this is not a requirement at this time. Detailed description of the listed steps is as follows.

a) VOMS-enable Keystone installation and configuration

The installation and configuration of VOMS-enable Keystone is available online[32]. That will enable X.509 authentication mechanism and allows users with valid VOMS proxy certificate to log in. The actual VO for EGI Cloud Federation fedcloud.egi.eu should be enabled in the configuration. There is an option for automatically creating new users for trusted VO on the fly.

b) OCCI installation and configuration

The steps of installation and configuration of OCCI is available online[33]. The installation and configuration should be done on the machine with Nova server. The OCCI implementation is not perfect; occasionally Nova server needs to be restarted for refreshing OCCI configuration (especially when new images are added).

c) Integration with accounting service APEL

Like RP with OpenNebula, the client for accounting service APEL must be installed and configured. The details of installation and configuration of APEL for Openstack is available at[34,35].

[29] https://wiki.egi.eu/wiki/Fedclouds_BDII_instructions
[30] https://wiki.egi.eu/wiki/GOCDB/Input_System_User_Documentation
[31] http://docs.openstack.org/install/
[32] http://keystone-voms.readthedocs.org/en/latest/index.html
[33] https://github.com/stackforge/occi-os
[34] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Scenario4

d) Integration with VM Image management infrastructure
Resource Providers are required to integrate their Openstack with an image management service used within the federation. Installation and configuration details are available online in the Wiki[36]. This service ensures that all images are trusted and up-to-date for all Resource Providers across the federation. In addition to vmcaster/vmcatcher, glancepush-vmcatcher[37] uses vmcatcher's event handler to signal glancepush that a new image was updated in vmcatcher's cache and glancepush will check and publish images from vmcatcher cache to glance service in Openstack.

e) Integration with information system LDAP/BDII
Integration with BDII for RP with Openstack is identical as in the OpenNebula case. The instructions are available online in the Wiki[38].

6.3 Synnefo

Synnefo (http://www.synnefo.org/) is open source cloud software used to create massively scalable IaaS clouds. It uses Google Ganeti for the low level VM management and also talks to the outside world through the OpenStack APIs with extensions for advanced operations. Synnefo in conjunction with Google GANETI (https://code.google.com/p/ganeti/) is the software that empowers GRNETs ~Okeanos service (https://okeanos.grnet.gr) that currently supports 2100 users with 2941 VMs and 10119 Virtual cores. ~Okeanos is only partially integrated with the Federated cloud infrastructure using snf-occi (http://www.synnefo.org/docs/snf-occi/latest/index.html), an implementation of the OCCI specification on top of synnefo's API kamaki. Development for the rest of the modules required is currently foreseen for the near future but due to lack of manpower and parallel developments of the synnefo API there is no estimate for the date of delivery for each module.

6.4 Other cloud management frameworks and public cloud providers

Within the federated cloud we have the rOCCI technology being provided and used currently to support the bridging to OpenNebula. The group are also working on the bridging to other private cloud software stacks using this method as well as investigating the possibility of using this for bridging to public cloud infrastructures.

[35] https://github.com/EGI-FCTF/osssm/wiki
[36] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Scenario8:Configuration#VMcatcher
[37] https://github.com/EGI-FCTF/glancepush
[38] https://wiki.egi.eu/wiki/Fedclouds_BDII_instructions

7 JOINING THE FEDERATED CLOUD

7.1 User Community

The EGI Federated Cloud is a seamless network of public and private clouds, built around open standards and focusing on the requirements of the scientific community. The result is a new type of research e-infrastructure, based on the mature federated operations services that make EGI a reliable resource for science. When using EGI Federated Cloud resources, researchers and research communities can count on:

- Total control over deployed applications
- Elastic resource consumption based on real need
- Immediately processed workloads – no more waiting time
- An extended e-Infrastructure across resource providers in Europe
- Service performance scaled with elastic resource consumption
- Single sign-on to cloud resources at multiple, independent sites

The typical user workflow for a user to get access to the EGI Federated Cloud from first registration to readying for deployment of VMs in a cloud provider is as below;

1. Obtain a grid certificate from a recognised CA.
2. Join a Virtual Organisation:
    a. The fedcloud.egi.eu Virtual Organisation (VO) provides resources for application prototyping and validation. The VO can be used for up to 6 month for any new user.
    b. Several other VOs of EGI make resources available from the Federated Cloud. Find a suitable VO in the Operations Portal. (Search for Cloud as a middleware type.)
    c. New VOs can be setup in the Operations Portal, and invite sites from the infrastructure to support them.
3. Reuse existing images from the Application Database Cloud Marketplace, or other repositories
    a. Using the command line client
    b. Using one of the high level brokering tools that are interoperable with the Federated Cloud
4. Prepare fully customised Virtual Appliances and deploy these to the sites:
    a. Prepare Virtual Machine Images (VMIs) that encapsulate your application. See the application porting tutorial below for tips.
    b. Make the VMIs available online, for example in the Stratuslab Marketplace
    c. Register the VMIs as Virtual Appliance in the EGI Applications Database
    d. Inform the Manager of your VO through Applications Database about the new Virtual Appliance. He/she will include your images in the VO-wide image list, so these will be deployed on the Federated Cloud sites of your VO.
    e. Use the command line client, or some high level environment, for example an Infrastructure broker or an Application Broker to instantiate and manage your Virtual Machine Images on cloud resources.

7.2 Resource Provider

EGI Federated Cloud resource providers are institutions and companies that contribute to the FedCloud providing access to their cloud infrastructure. Resource providers are free to use any Cloud Management Framework (OpenNebula, OpenStack, etc...), the only requirement is that the CMF exposes interfaces compliant to the FedCloud standards. These are not exclusive of other mechanisms and as such normally the standards are in addition to other interfaces and capabilities.

Every institution and company is invited to join the EGI Federated Cloud. The members of the EGI Federated Cloud have also the opportunity to join the EGI Federated Cloud Task Force, contributing directly to the creation and implementation of the clouds federation.

The information necessary from the resource provider is collected via the form as detailed below (fields with * are mandatory);

- Name*
- Institute*
- Email address*
- One paragraph long description of your organization
- Envisaged timeline (is there a deadline to finish the setup? for how long do you wish to contribute to the EGI Federated project?)
- Estimated number and size of machines that you may provide to EGI
- Type of Cloud Management Framework you are using
- Link to webpage, document or other online resource for further information.

The resource provider may then engage with the federated cloud group for everything from the assistance in setting up the underlying cloud management framework through to the configuration of the cloud service connectors that support federation. An important point of note is the autonomy under which the resource providers operate. This allows the federation of IaaS Cloud resources in EGI is built upon the extensive autonomy of Resource Providers in terms of ownership of exposed resources.

7.3 Technology Provider

We are supporting a number of different new technologies and technology types within the federated cloud and as such have no strict policy for technology providers to 'join' the federated cloud. We encourage their contact with the management of the fedcloud and then incorporate them into mailing lists etc on demand.

8 CONCLUSION

The Federated Clouds Task started exploring a federation of private institutional Cloud deployments with eight core scenarios to begin with, and later on extended these to ten scenarios (see section 2.1). The EGI Cloud Infrastructure Platform consists of deployments of different Cloud Management Frameworks (CMF) (OpenStack, OpenNebula,, WNoDeS and Synnefo) with varying levels of popularity. All these CMF whom have level of integration with the various core services to satisfy the certification procedure as defined. A number of other CMF are in existence and as such the Task is currently investigating the connection of this other platforms and supporting their integration to the same level as the current technologies. A number of pilot deployments with Research Communities stemming from within the EGI ecosystem and external to it have demonstrated the platforms support for typical research community requirements. This is allowing a significant growth in the number of research communities that are being supported with different models of utilisation being incorporated by each new group. This allows us to build a catalogue of operational and application design models with which we can engage further communities and discuss their needs.

This document allows a provider of cloud infrastructures for research to understand both the technical and policy requirements that are placed upon them by membership of the EGI Federated Cloud. Using the input from this document a provider can make a balanced decision on the type of cloud software they wish to deploy, how much work is required on top of the cloud installation procedure is needed to federate the cloud resource with others, and where the different other services that are needed to connect to the infrastructure are used within the federation. It has also been shown how the resource provider, to enhance the services they are able to provide, may broaden the types of research communities and applications that they are able to support.

This document also captures the state of the cloud federation at the end of the final development phase as the Federated Cloud moves towards a production infrastructure. This also shows how the external operations and structure for the support of services within EGI integrate with possible internal services that the provider may operate to support other communities outside of EGI. The experiences, changes to technologies etc. are all tested with real experiences by providers that have deployed the various different technologies that are described within this document.

The main goal of the Task is now to further mature and finalise the integration modules so that Cloud Resource Providers will be able to formally transition their Cloud Resources into EGI's production infrastructure as part of the EGI Cloud Infrastructure Platform.

9 REFERENCES

R 1	R. Nyren, A. Edmonds, A. Papaspyrou, and T. Metsch, “Open Cloud Computing Interface - Core," GFD-P-R.183, April 2011. [Online]. Available: http://ogf.org/documents/GFD.183.pdf
R 2	T. Metsch and A. Edmonds, “Open Cloud Computing Interface - HTTP Rendering," GFD-P-R.185, April 2011. [Online]. Available: http://ogf.org/documents/GFD.185.pdf
R 3	“Open Cloud Computing Interface - Infrastructure," GFD-P-R.184, April 2011. [Online]. Available: http://ogf.org/documents/GFD.184.pdf
R 4	SNIA Technical Position CDMI v1.0.2, March 2012. [Online] Available: “http://snia.org/sites/default/files/CDMI%20v1.0.2.pdf
R 5	R. Mach, R. Lepo-Metz, S. Jackson, L. McGinnis, “Usage Record – Format recommendation" GFD-P-R.98, September 2006. https://www.ogf.org/documents/GFD.98.pdf
R 6	GLUE Specification V2.0”, GFD-R-P.147, March 2009. [Online]. Available: http://www.ogf.org/documents/GFD.147.pdf