EGI FEDERATED CLOUD BLUEPRINT

Version	v3, 2015-03-24
Last reviewed by	Enol Fernandez/EGI.eu
Document Link:	https://documents.egi.eu/document/2451

Abstract

This documents describes the EGI CLoud Infrastructure Platform (CLIP) architecture. This platform is modelled around the concept of an abstract Cloud Management stack subsystem that is integrated with components of the EGI Core Infrastructure Platform. The document details the supported APIs and services for building the federated cloud and how these are integrated with the different core infrastructure components of EGI that every resource provider willing to join the federation should provide.

I. COPYRIGHT NOTICE

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[1], 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[2] for EGI Resource Providers that wish to securely federate[3] and share their virtualised environments as part of the EGI production infrastructure;
- Deploy a test bed[4] to evaluate the integration of virtualised resources within the existing EGI production infrastructure for monitoring[5], accounting[6] and information services[7];
- Investigate and catalogue the requirements[8] for community facing services based on or deployed through virtualised resources;
- Provide feedback[9] to relevant technology providers on their implementations and any changes needed for deployment into the production infrastructure;
- Identify and work with user communities[10] willing to be early adopters of the test bed infrastructure to help prioritise its future development;
- Identify issues[11] that need to be addressed by other areas of EGI (e.g. policy, operations, support & dissemination),
- Evolve the testbed into a production infrastructure.

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

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

2 FEDERATION MODEL

Federation of IaaS Resource Providers in EGI is built upon the extensive autonomy of Resource Providers in terms of ownership of the exposed resources. The EGI CLoud Infrastructure Platform (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). 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.

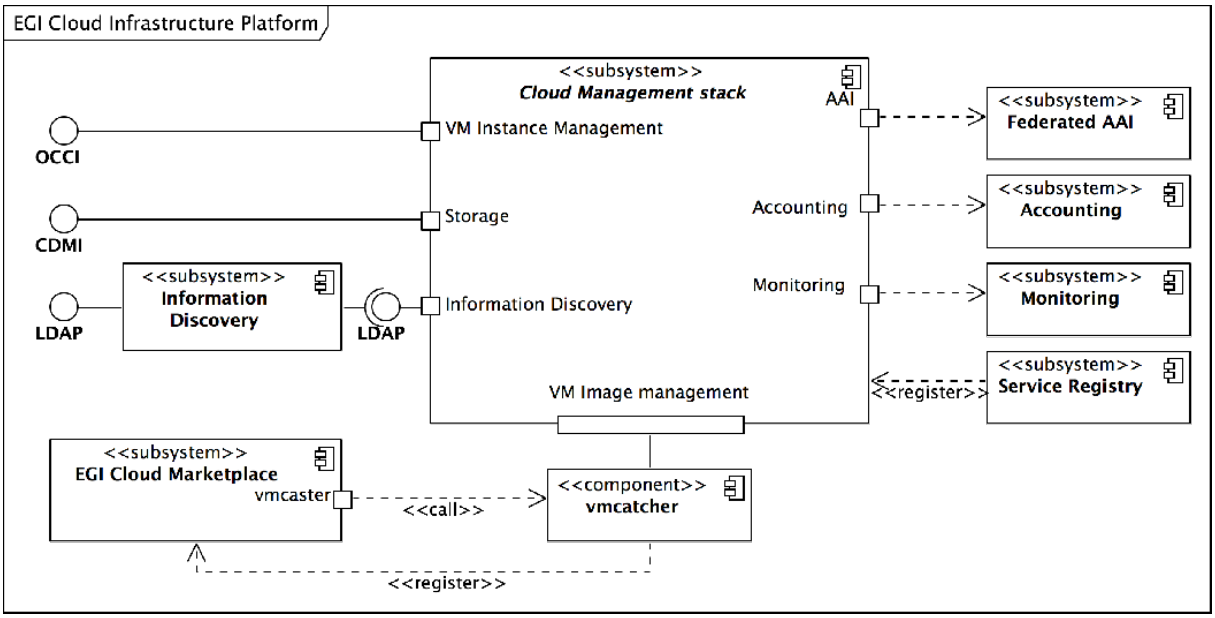

Figure 1: Architecture of the EGI Cloud Infrastructure Platform

The CLIP is 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, all of these must be realised by Cloud Management stack deployments:

- 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 integration with the EGI Cloud MarketPlace
- The integration with the EGI Information Discovery system

At the same time, the architecture defines two interaction ports for providing IaaS capabilities:

- The provisioning of VM management interface
- The provisioning of Object Storage interface

Local Cloud Management stack deployments must provide at least one of these IaaS interaction ports preferably using standardised APIs, namely OCCI for VM management, and CDMI for object storage. The Resource Providers may support other proprietary interfaces if the integration with the EGI Core Infrastructure and EGI Collaboration Platform is also provided for those interfaces.

Table 1 summarizes the current integration level with several Cloud Management stacks. The EGI Federated Cloud Task gives Resource Providers a platform to share their implementation solutions for a commonly deployed specific Cloud Management stack (e.g. OpenNebula and OpenStack). Through this collaboration, Resource Providers gradually develop and mature deployment and configuration profiles around common Cloud Management stacks. 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.

Cloud Mgmt. Stack	Integration					
	Fed. AAI	Monitoring[13]	Accounting	Img. Mgmt.	OCCI	CDMI
OpenStack	Yes	Yes	Yes	Yes	Yes	Yes
OpenNebula	Yes	Yes	Yes	Yes	Yes	-
Synnefo	Yes	Yes	-	-	Yes	Yes

Table 1: Overview of available integration for deployed Cloud Management Frameworks

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

3 EGI CORE SERVICES FOR CLOUD

EGI Federated Cloud Resource Providers integrates into the EGI infrastructure with a set of core services: AAI, information discovery, central service registry, monitoring, accounting and VM image management. This section describes the required integration for each of these services.

3.1 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). The EGI Cloud Infrastructure Platform currently also uses VOs for authorization and authentication. Three VOs must be supported at every Resource Providers:

- *ops* VO, used for monitoring purposes;
- *dteam* VO, used for testing purposes by site operators; and
- *fedcloud.egi.eu* VO, a catch-all VO that provides resources to users for a limited period of time (6 months initialliy) for prottpying and validation.

Resource Providers may support additional VOs in order to give access to other user communities.

EGI Federated Cloud members have developed integration modules for each Cloud Management stack. 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 and thus creates a local VOMS proxy certificate. The VOMS proxy certificate is used 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.

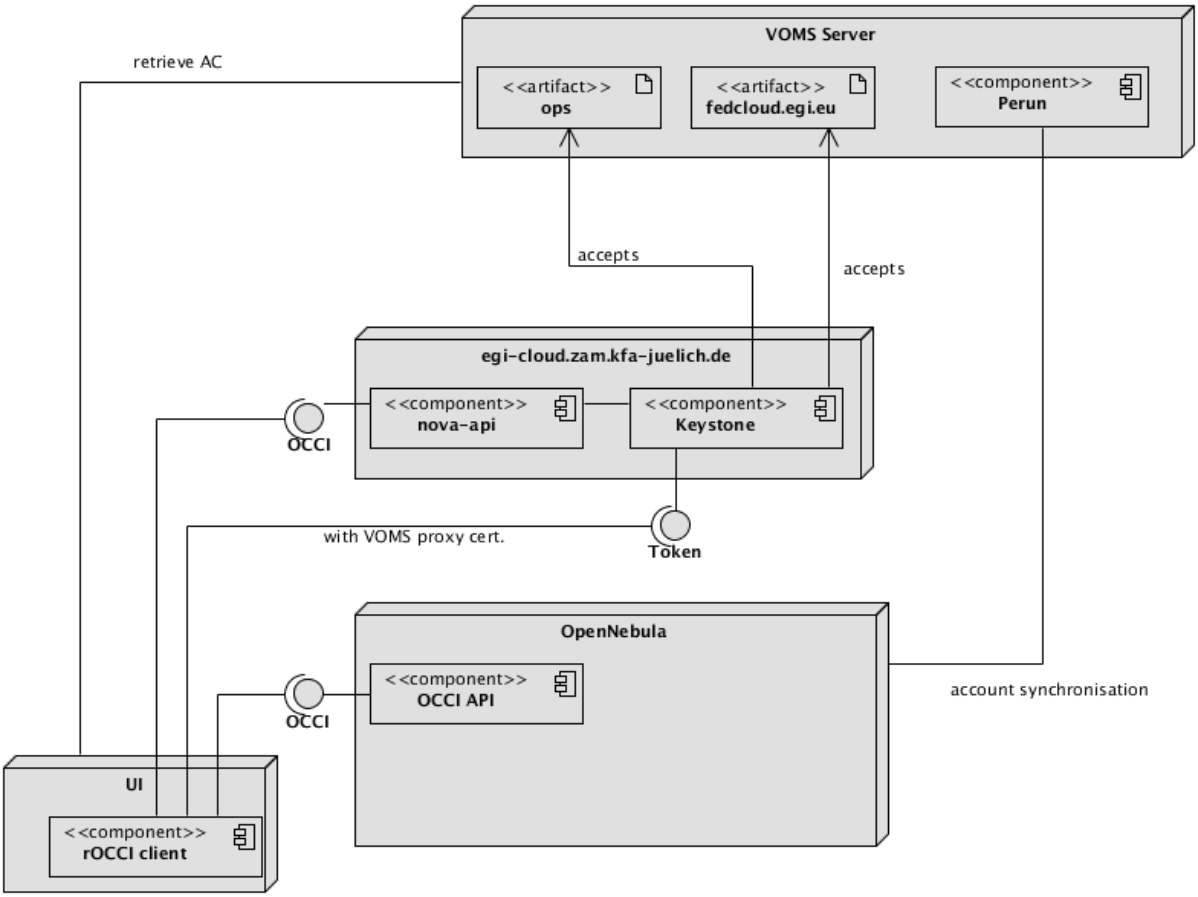

Figure 5: Model of the Federated Cloud authentication architecture

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.
- Synnefo implements the Keystone API as described above.

3.2 Information discovery

Users and tools can discover the available resource in the infrastructure by querying EGI information discovery services. The common information system deployed at EGI is based on the Berkeley Database Information Index (BDII) with a hierarchical structure 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 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.

Resource Providers must provide a Site-BDII endpoint that published information on the available resource following the GLUE2 schema. 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.

EGI provides an implementation for service-level information that generates information supporting OpenStack and OpenNebula Cloud Management Frameworks; Synnefo support is currently being added[14]. The information is published in a different subtree (Glue2GroupID=cloud) so it can coexist with grid information and is easily discoverable by users.

3.3 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 are available in GODCB:

- eu.egi.cloud.accounting
- eu.egi.cloud.storage-management.cdmi
- eu.egi.cloud.vm-management.occi
- eu.egi.cloud.vm-metadata.marketplace
- eu.egi.cloud.vm-metadata.vmcatcher
- eu.egi.cloud.vm-metadata.appdb-vmcaster

Higher level broker services also have its own service types:

- eu.egi.cloud.broker.compss
- eu.egi.cloud.broker.proprietary.slipstream
- eu.egi.cloud.broker.vmdirac

There is an additional service type (eu.egi.cloud.information.bdii) which was used at the early stages of the Federated Cloud but is no longer needed for production. It might be removed in the future.

3.4 Monitoring: SAM

Services in the EGI infrastructure are monitored via SAM (Service Availability Monitoring). Specific 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 (eu.egi.cloud.OCCI-VM): Creates an instance of a given image by using OCCI, checks its status and deletes it afterwards.
- Accounting probe (eu.egi.cloud.APEL-Pub): Checks if the cloud resource is publishing data to the Accounting repository

[14] https://github.com/enolfc/cloud-bdii-provider/tree/synnefo_support

- TCP checks (org.nagios.Broker-TCP, org.nagios.CDMI-TCP, org.nagios.OCCI-TCP and org.nagios.CloudBDII-Check): Basic TCP checks for services.
- VM Marketplace probe (eu.egi.cloud.AppDB-Update): gets a predetermined image list from AppDB and checks its update interval.
- Perun probe (eu.egi.cloud.Perun-Check): connects to the server and checks the status by using internal Perun interface

Probes for CDMI and the image synchronization mechanism are currently under development.
More information on cloud probes can be found here: https://wiki.egi.eu/wiki/Cloud_SAM_tests. Currently 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 by following EGI's "Adding new probes to SAM" procedure (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 following SAM tests were added to operations tests:

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

3.5 Accounting

EGI Federated Cloud has agreed on a Cloud Usage Record -which inherits from the OGF Usage record [R5]- that defines the data that resource providers must send to EGI's central Accounting repository. The Usage Record contains the following fields (currently under review):

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)	
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	

Support for retrieving the accounting data in this format is available from:

- OpenNebula – https://github.com/EGI-FCTF/opennebula-cloudacchttps://github.com/EGI-FCTF/opennebula-cloudacc
- Openstack – https://github.com/IFCA/caso is a new implementation that substitutes the previous existing ones (https://github.com/EGI-FCTF/osssm and https://github.com/schwicke/ceilometer2ssm). The transition to the new implementation is expected to be performed in early January 2015.
- Synnefo provides its own internal component.

Once generated, records are delivered via the network of EGI message brokers to the central accounting repository using APEL SSM (Secure STOMP Messenger) provided by STFC. SSM client packages can be obtained at http://apel.github.io/apel/. Further details on SSM configuration may be found at https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Scenario4#Publishing_Records. A Cloud Accounting Summary Usage Record has also been defined and summaries created on a daily basis from all the accounting records received from the Resource Providers are sent to the EGI Accounting Portal. The EGI Accounting Portal also runs SSM to receive these summaries and provides a web page displaying different views of the Cloud Accounting data received from the Resource Providers[15].

3.6 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

[15] http://accounting-devel.egi.eu/cloud.php

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.

The EGI Applications Database (AppDB for short) and HEPiX image lists[16] subscribers at the Resource Providers provide the principal functionality of this subsystem.

In general, the EGI AppDB[17] 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. One of the most significant features offered by the service is the 'Cloud/Virtual Appliances Marketplace'[18] section, to support the uptake of EGI's new production infrastructure, the Federated Cloud.

The new marketplace section enables the sharing of Virtual Appliances (VAs) — 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. The VA themselves are stored in distributed appliance repositories that are provided and managed elsewhere, typically by the Research Community itself. A catch-all appliance repository is available[19].

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 HEPiX image lists which Resource Providers can subscribe to. AppDB facilitates the job of creating these image lists directly from the portal for any given VA or VO-wide image lists that contain several VAs for a VO. AppDB also queries the EGI Information service to display which Resource Providers are actually providing the VA and the usage details for instantiating it.

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

[16] https://github.com/hepix-virtualisation/image_list_format_docbook
[17] https://appdb.egi.eu
[18] https://appdb.egi.eu/browse/cloud
[19] http://appliance-repo.egi.eu

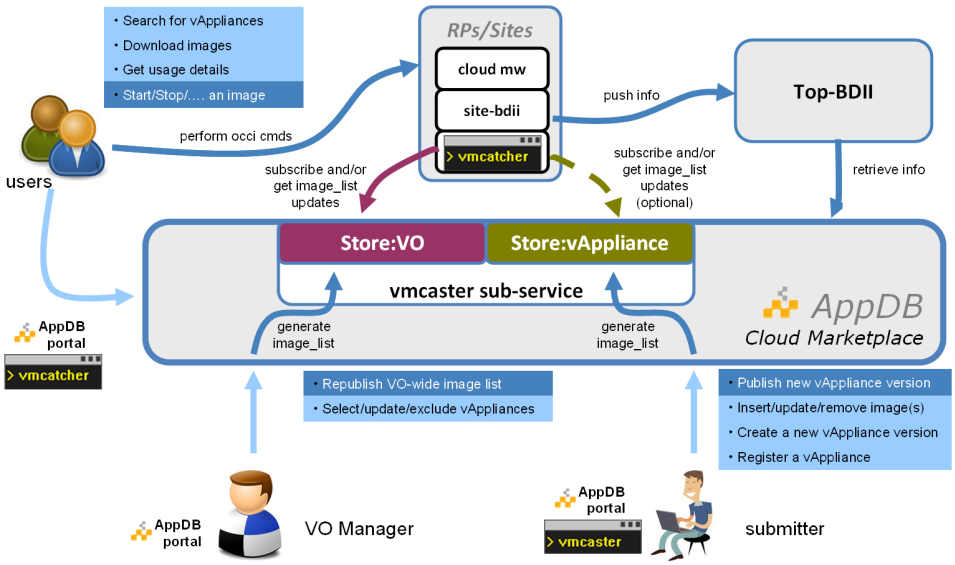

Figure 7: Using the EGI AppDB as Virtual Appliance Marketplace.

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, the site administrator (using vmcatcher tool or any other tool supporting HEPiX image list format):

- 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 Management stack the site maintains

updates the information system of the infrastructure.

4 CLOUD SPECIFIC INTERFACES

Resource Providers can participate in EGI Federated Cloud by supporting one or several of the following ports:

- IaaS VM management
- IaaS Storage management

EGI Federated Cloud promotes the use of standard interfaces for providing the services: OCCI for VM management and CDMI for storage management. Both have open implementations for the main Cloud Management stacks in EGI Federated Cloud and are fully integrated with the EGI Core Platform.

However, Resource Providers are welcome to deploy and offer additional services or APIs to the Federation as long as they are integrated with EGI core services as described in previous sections. The integration steps are defined in EGI PROC19[20]. This procedure will assure that any new interface will meet the following criteria:

- Usage of resources must be recorded and integrated in the EGI Core Accounting system.
- The status of the service must be monitored via the EGI Core Monitoring system.
- VM images of the supported VOs in EGI VM Marketplace must be available at the Resource Provider through the VM management API.
- Information on the service must be available through the EGI Information Discovery system.
- Resources can be accessed through the EGI resource allocation

A brief description of the currently supported APIs is given in the following sections.

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/.

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

[20] https://wiki.egi.eu/wiki/PROC19

migration. The concept of mixins is used to facilitate extensibility and provide a way to define provider-specific features.

4.1.1 rOCCI framework

In the Federated Cloud environment, OCCI is deployed as a variety of platform-specific implementations. The rOCCI framework (funded by an EGI-InSPIRE mini-project[21]) aims to provide a common implementation to further improve interoperability between different Cloud Management stacks.

rOCCI-server supports different backends that interact with specific Cloud Management stacks. OpenNebula is the main supported backend in rOCCI, but Amazon EC2 and Microsoft Azure are also on development (with EC2 backend currently in testing phase)[22].

4.1.2 OCCI extensions for FedCloud

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.). OCCI v1.1 (current version of the standard) lacks of mechanisms to allow this contextualization of VMs, hence we have proposed the use of a new OCCI mixin that has an attribute to hold user-provided data that contains the context information for the VM. More information on the mixin is available at EGI's wiki[23].

Each Cloud Management stack provides its own mechanisms to make these data available at the VM. FedCloud recommends using cloud-init[24] for this handling the data. 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.

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.

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 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.

[21] TSA4.4 Providing OCCI support for arbitrary Cloud Management Frameworks
[22] See https://wiki.egi.eu/wiki/ROCCI-server_Backend_development_status
[23] https://wiki.egi.eu/wiki/Fedcloud-tf:WorkGroups:Contextualisation#OCCI_support
[24] https://launchpad.net/cloud-init

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.

4.2.1 CDMI in FedCloud

For the Federated Cloud environment, the primary goal of CDMI is to offer a standard interface for operating with blob data. Currently there is a CDMI plugin available for OpenStack Swift that is able to profit from the Keystone VOMS support for Authentication and Authorization.

5 FEDERATING CLOUD RESOURCES TO EGI

This section details the methodology to integrate and adapt a Cloud Management stack to become a Resource Provider in the EGI Federated Cloud. 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. With the infrastructure currently in production, now a certification process[25] allows official membership.

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, a temporary Cloud Resource Center Registration and Certification procedure was created[26]. This was to detect steps in the existing procedure 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. The testing phase is now over and a single procedure for certifying Resource Centers is now in place (https://wiki.egi.eu/wiki/PROC09).

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. 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.

Full information on how to integrate a new Resource provider into the Federation is available in the wiki as MANUAL 10: https://wiki.egi.eu/wiki/MAN10

[25] https://wiki.egi.eu/wiki/PROC09_Resource_Centre_Registration_and_Certification

[26] https://wiki.egi.eu/wiki/PROC18

6 JOINING THE FEDERATED CLOUD

6.1 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 clienthttps://wiki.egi.eu/wiki/Fedcloud-tf:ROCCI-Client_Usage
    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 EGI appliance repository
    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.

6.2 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.

New sites should follow EGI Certification Procedure as described in https://wiki.egi.eu/wiki/PROC09. Existing sites may add services to their current offer following the documentation available in the wiki

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.

6.3 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.

Technology Providers that want to integrate their developments in the production infrastructure must follow EGI PROC19[27].

[27] https://wiki.egi.eu/wiki/PROC19

7 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 Appendix). The EGI Cloud Infrastructure Platform consists of deployments of different Cloud Management Frameworks (CMF) (OpenStack, OpenNebula 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 current state of the cloud federation as 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.

8 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.pdfhttps://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

9 APPENDIX: 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.

9.1 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. 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.

9.2 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

9.3 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)

9.4 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?)

9.5 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?

9.6 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?

9.7 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.

9.8 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.

9.9 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.

9.10 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