

EGI Cloud Integration Profile

Version 7

4 April 2011

Steven Newhouse & Michel Drescher, EGI.eu

Abstract

The purpose of this document is to define a technical roadmap for the interoperable integration of virtualised resources from different resource providers to provide an integrated federated virtualised resources infrastructure for exploitation by EGI's user community. To achieve interoperability between the individual deployments, while allowing individual sites the flexibility to deploy the software that they wish, some interfaces will need to be constrained to clearly defined specifications.

This document defines a minimal set of usage scenarios that when supported will provide key functionality for the end-users wishing to utilise 'cloud' interfaces provided as part of EGI. From these scenarios a number of functional areas are defined and from these functional areas a set of standards and specifications are identified that will define interaction across this functional areas.

These scenarios and specifications are identified to promote discussion amongst the end-user community (as a starting point for their use) and for resource-providers (to verify the deployability of these interfaces). There will be follow on discussion within the TCB, NGIs interested in engaging in these developments, that will be the main focus at the User Virtualisation Workshop to be held in Amsterdam 12-13th May 2011.

Document Status:	**DRAFT**
Dissemination Level:	**PUBLIC**
Document Link:	https://documents.egi.eu/document/435

Issue	Date	Comment	Author/Partner
1	30-03-2011	First draft	Michel Drescher, EGI.eu
2	31-03-2011	Updated document style, incorporated 1st review.	Michel Drescher, EGI.eu
3	31-03-2011	Finished incorporating 1st review	Michel Drescher, EGI.eu
4	02-04-2011	Added sections on the overall architecture, EGI Cloud Profile etc.	Michel Drescher, EGI.eu
5	03-04-2011	Abstract, Motivation, Context chapters	Steven Newhouse, EGI.eu
6	04-04-2011	Service deployment, etc.	Michel Drescher, EGI.eu
7	04-04-2011	Final review before first publication, image polishing	Steven Newhouse, Michel Drescher, EGI.eu



TABLE OF CONTENTS



1 Motivation

EGI is faced with a number of challenges:

- Significantly expanding EGI's user community will require different software environments that are currently provided.
- Many of EGI's existing and potential future user communities are expecting to access distributed computing resources in an 'Infrastructure as a Service' (IaaS) usage model.
- Delivering these distributed services as an integrated federated IaaS model.

Within this model it is very unlikely that all sites will deploy the same software. Therefore, to ensure that the individual deployments can be accessed consistently by end-users, or more likely by experts acting on their behalf, some constraints are necessary on the interfaces and their mode of operation that are exposed for general use.

The interfaces that define these constraints are defined as the 'EGI Cloud Profile'. This profile is currently defined in terms of specifications and emerging standards that are recognised or becoming recognised in the wider community. It is expected that this profile will evolve over time – as new specifications and standards emerge or old ones are deprecated – and as interfaces are recognised as needing to enter or leave the profile.

Development of this profile will be as a result of feedback from various communities gathered through the mechanisms identified below.

- Resource Providers through the Operations Management Board
- End-Users through the User Community Board
- Technology Providers through the Technology Coordination Board (which will formally 'own' the EGI Cloud Profile)
- General feedback from the community at the User and Technical Forums
- Specific feedback through dedicated workshops, such as the EGI User Virtualisation Workshop being held 12-13th May 2010 in Amsterdam (http://go.egi.eu/uvw1)

It is expected that this profile will be contributed into discussions taking place in the Open Grid Forum and other organisations to form a Cloud Interoperability Profile that is recognised by other academic resource providers around the world.



2 Context and Boundary Conditions

Clearly, there are many usage scenarios that a federated virtualised infrastructure could support. The purpose of this document is to define a ***minimal*** set of scenarios that can provide a basis for higher-level functionality at a later date. The following scenarios relate to:

- Running a virtual machine image that is provided by the remote site.
- Running both a virtual machine image with data that I have uploaded to a site.
- Selecting which resource provider from several to use.
- Being able to account for resources used by an individual across multiple resource providers
- Allow a resource provider to publish the availability and reliability of its resources.

The move to a federated virtualised infrastructure must require minimal changes to the existing production infrastructure. Therefore elements of the existing operational infrastructure will be reused (unless proven not to work) including:

- The existing BDII will be used to distribute information about the virtualised environment provided by the resource provider
- The existing X.509 based authentication credential will be used by those accessing the virtualised environment
- VOMS will be used to provide the authorisation mechanism for those able to access a resource provider
- The existing message bus infrastructure will be reused
- Accounting records will reuse the existing accounting infrastructure (message brokers, central database and portal), which is already being adapted to support virtualised resources in PY2.

To scope down the activity in this initial phase there are a number of areas defined as being out of scope. These are recognised as relevant areas for study, but are not seen as a priority at this moment:

- Service Level Agreements: Ultimately users need to be assured of the resources that they have access to and compensation rules if these are breached. However, at this stage a simple expectation of CPU, memory and duration is probably sufficient.
- Higher Level Services: Managing the provisioning of the desired infrastructure across multiple resource providers will need to be automated once the size of the desired infrastructure and the number of resources available for use increases. However, significant results can probably be achieved initially with a manual approach.



3 Scenarios and Use Cases

"The hardest part of any journey is taking that first step." – Unknown

This part of the document introduces a set of use cases and scenarios, starting from very simple to more complex user stories that are typical for Cloud Computing in EGI. Each of the scenarios described in this section build on top of each other as the complexity grows. Overall, their goal is to provide the framework and constraints within which EGI's Cloud Computing profile is designed to ensure interoperability between the resource providers federated in EGI.eu

Each scenario described below is introduced with one or more archetypical statements that indicate the scope and complexity of the described scenario.

Encoded within the statements are a number of assumptions that are further explained thereafter.

Following, a section describes the services that must be deployed in the operational infrastructure to implement and support the respective scenario.

Wherever possible, public and mature standards are identified to facilitate interoperability in the federated virtualised infrastructure. Where appropriate standards are not available, suitable existing software products are listed on which the integration and interoperability is required to take place. In this case, a clear need for standardisation in this area is implied in the description.

Where applicable and identified a set of open issues are described, indicating areas for discussion with and by the major stakeholders of this profile.



3.1 Scenario 1: Running a pre-defined VM Image

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

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

3.1.1 Assumptions

The statements given above insinuate a certain service offering as depicted below:

- The user already knows the specific VM image she would want to instantiate.
- The VM image is clearly identifiable and with that selectable through whichever means by the user.
- The VM image already resides within the remote resource provider and is ready for instantiation.
- The resource provider will allow multiple users access to the same basic VM image.
- Access to particular VM image may be restricted to specific users.
- A federated identity infrastructure is in production that can be used to access the resource
- A particular format for VMs is not required as the execution of the VM is local to the selected virtualised resource provider.
- Taking a snapshot of a VM for later restart is not supported in this scenario.

From the assumptions, and the depiction of the scenario above a certain number of required services and interfaces can be derived.

3.1.2 Services

3.1.2.1 Management Interface

A management interface is necessary for two key roles in this scenario. The user must be able to start and stop the VM as he sees fit, hence access to the image and instance must be guaranteed; and the resource provider needs to manage the VM image to efficiently manage its resources (for example, migrate the VM instance to prevent resource over-use).

3.1.2.2 Authentication & Authorisation

The user's preferred authentication provider must be integrated into the infrastructure management, and interfaced so that the user's identity may be solicited when interacting with the VMM. Based on the user's identity and associated attributes (that may be provided by the same authority, or a different attribute authority) a series of authorisation decisions must take place between the user accessing the VMM initially, and the actual instantiation of a VM image.

3.1.2.3 Remote Network access

Instantiating a VM has not much use when it cannot be accessed while executing. Therefore some sort of network access from outside the resource provider's site to the running VM must be enabled (i.e. externally visible IP address) must be needed to provide:

- Upload input data into the running VM instance
- Execute applications installed within the VM
- Download output data.

3.1.3 Standards

3.1.3.1 Management Interface

OCCI provides a mature model and implementable rendering for the management of VMs. OCCI provides operations to categorise, identify (includes discovering), connect/link, and operate resources of various kinds.

3.1.3.2 Authentication & Authorisation

SAML provides a framework upon which a number of identity providers (for federated identity), attribute authorities (for federated role and group based assessment) and resource providers can integrate. Existing X.509 based PKIs provide strong end user identity hence should be integrated through a bridging mechanism translating X.509 subject information into appropriate SAML tokens.

XACML is a framework suitable for formulating both simple and complex policies that help rendering authorisation decisions.

3.1.3.3 Remote Network Access

Access to the VM instance from outside the resource provider's site will take place through an IP address provided by the resource provider. The network access may range from very simple, command line based access to complex GUIs with interactive access to applications running within the VM and is not defined or constrained by this scenario.



3.2 Scenario 2: Running my data and VM in the Infrastructure

This scenario includes scenario 1, plus the following statements:

"I want to start a single VM instance 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"

3.2.1 Assumptions

The statements given above insinuate a certain service offering as depicted below:

- The user wants to upload their VM image to the remote resource provider before instantiation.
- The user also wants to download the VM image (or the snapshots of it) from the cloud to local data storage.
- The data that the applications within the VM operate on is not stored within the VM image itself, but somewhere within the same resource provider.
- The VM image and the data must be linked as a configurable dependency

From the assumptions, and the depiction of the scenario above a certain number of required services and interfaces can be derived in addition to those mentioned in previous scenarios.

3.2.2 Services

3.2.2.1 Data staging

The user must be given the option to upload a VM image to the resource provider so that it appears as a selectable VM in the IaaS management interface (as described in scenario 1). The service must also allow downloading the selected VM image into local data storage.

3.2.2.2 Instance/image configuration

The user must have the possibility to configure the VM so that the data they have uploaded to the resource provider must be accessible to the applications within the Virtual Machine. Both image configuration (before instantiation) and instance configuration (while executing) must be supported.

3.2.3 Standards

3.2.3.1 Data staging

Many possible standards exist in this field. For the actual transfer of VM images or packages (see below), existing standards include the very popular GridFTP standard, or other massively scalable data transfer protocols.



The management of data in the cloud may be solved with implementations of CDMI and/or SRM, integrated with the authentication and authorisation frameworks based on the standards described above.

3.2.3.2 Instance/image configuration

For the description and configuration of the VM itself OVF is a viable solution. OVF defines a format for packaging and distribution of (collections of) VMs. This includes configuration of a VM, for example for data sets to be available at runtime.

3.2.4 Open issues

The assumptions in the scenario leave a number of questions open as described below:

- When deciding for a (set of) standards to integrate compute clouds and data clouds, what are the preferred, required, minimal options to make the data actually available to the user? Are applications within the VM required to implement, for example, CDMI clients to be able to access the data? Or should the integration point at/within the VM be defined to be a mount point within the VM's file system, perhaps as a driver implementing POSIX?
- How is the data scenario exactly scoped? Is the data pre-staged from the remote cloud storage into the compute cloud before the VM is instantiated? Or will the data be accessed at runtime? Is the data and the VM image pushed to the resource provider by the client before startup or pulled into the resource provider as part of the startup.

3.3 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."

3.3.1 Assumptions

The statements given above indicate several new features in this scenario:

- EGI's virtualised infrastructure is composed of many different resource providers.
- However, it does *not* imply that Resource Providers are identical, i.e. clones in terms of offered functionality. Different Resource Providers may offer different sets of VEEs and VMM interfaces and capabilities provided they abide the constraints defined in the EGI Cloud Profile.
- For different offerings from resource providers to be of any meaning to the user, the detailed service descriptions must be comparable in terms, units and language.
- Last, but not least, to compare offerings potentially large in numbers and complexity, the offerings must be easy to find, compare and available.

3.3.2 Services

3.3.2.1 Service Description

The service offerings of the EGI's federated resource providers must be consistently described and published. Publicising the offerings will be done individually per resource provider and as an infrastructure. These may be aggregated from other different perspectives.

Service descriptions spanning resource providers federated in EGI are likely to be complex in richness and diversity of the supplied information, but also in sheer amount of data being published. The identified solution therefore must be scalable and efficient in expressiveness of service descriptions and dissemination of information.

3.3.3 Standards

3.3.3.1 Service Description

The GLUE2 standard provides sufficient granularity to start describing service offerings of resource providers. Although originating from classic Grid environments, GLUE2 provides enough extension points and flexibility in its model to describe other service offerings as well.

Aggregation and collection of service offerings may be accomplished using RSS with XML integration, covering updates on service offerings and subsequent processing and aggregation at various subscribers to RSS feeds of the resource providers. Rendering into web pages suitable for human consumption may



be accomplished with XSLT functions shared across resource providers transforming technical GLUE2 XML representations of their service offerings into HTML/XHTML for website presentation.

3.3.4 Open issues

The assumptions in the scenario leave a number of questions open as described below:

- Definition of the GLUE2 objects needed to represent the virtualised environment.



3.4 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."

3.4.1 Assumptions

As with every scenario provided, there are several assumptions encoded in this scenario, too:

- The scenario statements do not stress the execution of a single VM. They are silent about this, so the execution of more than one VM at the same time must be considered a requirement for this scenario. A unique identifier (supplied by the client) is needed to correlate usage across multiple sites as part of the same activity.
- Usage of resources (CPU, RAM, I/O, data, etc.) needs to be accounted for across multiple resource providers – this requirement has been silently assumed to be present in all other scenarios described above. The important step forward in this scenario is that all accounting data is not considered an "implementation detail" anymore. Accounting data must be injected into the existing infrastructure in a consistent way across different implementations and hardware.
- Resource providers agree and follow the same rules for accounting the resource usage. The same units must be used when metering the same resource, and identical sensor points must be used when installing the metering points in the infrastructure.

3.4.2 Services

3.4.2.1 Accounting

The existing accounting infrastructure is used to transport and correlate the extracted uniformly formatted data for further aggregation. The exact mechanism as to how the individual usage is extracted and converted to an accounting record is implementation specific and out of scope of this document.

3.4.3 Standards

3.4.3.1 Accounting

Several public standards, and extensions to them, exist. OGF UR 1.0 provides the starting point for interoperable accounting data. UR 2.0 is chartered to include accounting for storage and service accounting. An extension/refactoring of UR is gauged towards Cloud specific interoperable usage accounting data, provided by the UK NGS as "UR+".

3.5 Scenario 5: Reliability/Availability of Resource Providers

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."

3.5.1 Assumptions

The statements given above insinuate a certain service offering as depicted below:

- Information about availability, reliability and the current status are provided by the resource provider as is. Independent rating, monitoring or reputation mechanisms are out of scope.
- The statement given above combines two aspects of operational performance of resource providers: a) historical data about past status information aggregated over time, and b) current status
- Availability and status information are therefore required to be interoperable/comparable between the individual resource providers, as they will be aggregated at multiple levels.

3.5.2 Services

3.5.2.1 Monitoring

To report the current status, and historical information of availability, a monitoring infrastructure must be in place at each resource provider. The monitoring infrastructure must take measurements at the same intervals, and units across all resource providers.

3.5.2.2 Reporting

The monitored data is of no use if it is not reported somewhere. The availability data needs to be properly aggregated before publication, and disseminated to the publication endpoints.

3.5.3 Standards

3.5.3.1 Monitoring & Reporting

No publically developed standard is available that would sufficiently describe interfaces of the monitoring infrastructure.

The infrastructure employed for service description (i.e. GLUE2 etc.) may be re-used to propagate information about the virtualised resource.

Extensive experience is available with a distributed Nagios infrastructure employed for service monitoring in EGI's federated distributed computing infrastructure.

3.5.4 Open issues

- Reporting availability is merely a function of integral aggregation of service outages over a given period of time – a profile or particular slice of common and generic accounting data. Information generated locally may also be injected into the existing site monitoring infrastructure.



3.6 Scenario 6: VM/Resource state change notification

This scenario includes scenario 4, plus the following statements:

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

3.6.1 Assumptions

- This scenario enables two management patterns: a) Reactive management caused by unforeseen incidents, such as sudden service outages, and b) Proactive management in terms of risk mitigation.
- This allows the resource provider to notify interested parties about changes in the user's VM state or a proposed state change in the VMM.
- It enables the end-user (and others) to build automated VM management and reactive workflows in user space.
- However, unlike scenario 5, this scenario implies clear, yet unspecified time constraints on the delivery of the status changes.

3.6.2 Services

3.6.2.1 Notification

A notification infrastructure needs to be deployed. This includes the definition of semantics of notification messages, both for reactive and proactive status updates. Notification patterns (e.g. immediate, time-constrained, volume-constrained, time/volume multiplexed, etc.) must be made available to the user, and actual transport mechanisms for the service and the user must be agreed upon.

3.6.3 Standards

A wide variety of notification message formats exist, and based on the formulated requirements an existing format may be easily picked.

Also a variety of transport mechanisms are available, whether standardised, industry standards, de-facto standards or proprietary. RSS feeds, Email, SMS, or common messaging mechanisms such as JMS, are available.

An interesting hybrid worth investigating is the emerging AMQP standard, which standardises on the wire representation of a message including the necessary routing information.

4 EGI Federated Cloud Architecture

The scenarios outlined in section 3 already give an indication on the focus of the EGI Cloud Architecture. From the perspective of this document, EGI federates resource providers into a consistent, interoperable, yet differentiated set of resource providers running virtualised environments accessible to authorised individuals across Europe. By adopting the NIST definition of Cloud Computing [R 1], EGI scopes the composition of its Cloud architecture as described in this section.

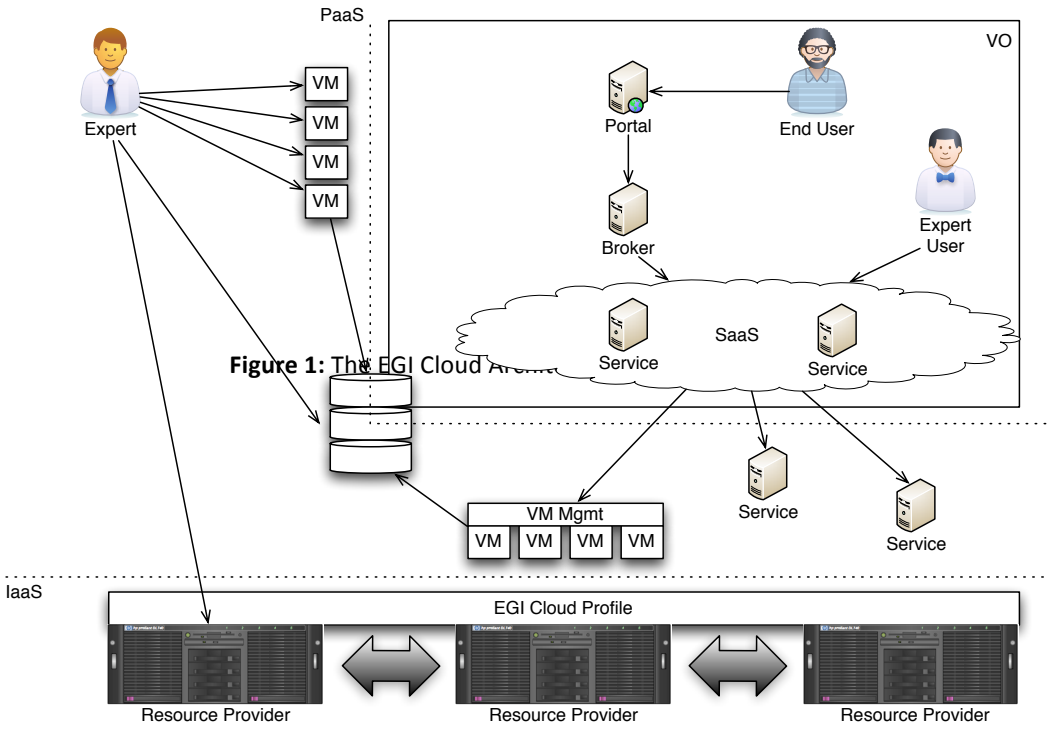

Figure 1: The EGI Cloud Architecture

The composition of EGI as a federation of resource providers demands a Cloud architecture that ensures a certain level of resource provider autonomy and freedom yet requires interoperability within the federation. When federated within EGI, parts of the resource provider's infrastructure will be bound by operational agreements, effectively creating a hybrid cloud across Europe. Considering the vast diversity of EGI's user communities with different, at best identical but at times detrimental requirements towards computing resources, an obvious if not natural approach to a harmonised service offering is to virtualise the federated infrastructure into a common *Infrastructure as a Service* towards the likewise federated user communities within EGI.

The chosen model as illustrated in Figure 1 allows separating concerns of business and areas of expertise between domain experts as follows. It is these domain experts that create the VM images that are needed to provide the services needed by end-users. These VM images are certified and placed into an image repository for deployment onto the infrastructure. The instantiated images provide a platform of services that can meet the needs of a particular user community (such as High Energy Physics, Social Sciences and Humanities, etc.) – which may include the deployment of a *Software as a Service* usage models – on top of a generic virtualised infrastructure.

4.1 Virtualising the infrastructure

Resource Providers federated within EGI provide a virtualised infrastructure, using a set of core services deployed within and across the federated resource providers, building a homogeneous fabric upon which its consumers may build their own respective domain specific infrastructure.

This core set of services and interfaces are necessary for any cloud provider to develop a service offering, and efficiently operate the infrastructure towards a consolidated and homogeneous access interface for its consumers. This set of services will be the same for all federated resource providers, and identical interfaces allow consumers to develop and build highly distributed platforms and applications, scaling across all resources EGI provides.

This is the EGI Cloud Profile described in this document, which reuses the basic operational infrastructure provided within EGI.

4.2 Consolidated platform offerings

Cloud computing experts proficient in building higher-level appliances use the EGI cloud infrastructure to provide higher-level services, applications and hosting environments as consolidated platform offerings to communities with related requirements and use cases for computing resource usage.

Platforms offerings built on top of a virtualised infrastructure are expected to vary greatly in shape or form. Platform offerings may include sophisticated application hosting environments, similar to Google App engine, or Salesforce.com's hosting platform. This service platform model involves the operation and maintenance of services that partially, or entirely, may run on the virtualised infrastructure provided by EGI.

The other end of envisioned platform offering models may include the development and provisioning of several strands of VM images providing a consolidated and integrated set of applications providing a software platform similar to platforms offered by common Linux distributions. Effectively a sophisticated and automated management and maintenance of Virtual Machine baselines that may be forked off of each other, those VM platforms (as opposed to service and application platforms which considered an "active" platform offering) can be seen as more and more constrained or profiled towards the target domain, the closer the application profile installed within the VM matches the final and complete application profile defined by the target community. For example, one structuring of VM image baselines



may align with the current organisation of scientists in Virtual Organisations (VO), and Virtual Research Communities (VRC), maintaining three layers of VM image baselines: a) A baseline of VM images that can be used for all targeted communities, from which b) VM images are derived that may support several VRCs, and finally c) VM image baselines supporting one or more Virtual Organisations. The platform provider customers then may use those highest profiled VM images to build the final services geared exactly towards their end-users needs.

Providing platforms as a service is the most flexible and least clearly defined area of Cloud computing, and many different models, separated or mixed, are expected to evolve. All but two envisioned models of providing platforms of higher-level organisation to customers are indicated in this section.

4.3 High-level user orientated services

The overall goal of the Cloud computing model described in this document is to enable the end user, whether citizen researcher or experienced and technology-apt, to focus on solving the problem at hand, instead of spending time maintaining the software infrastructure necessary to execute the highly specialised applications and tools geared towards their problem domain.

The fundamental distinction between citizen users and expert users lies in how they access the software portfolio presented. While expert users may automate the processes they engage in their daily work to solve the problems at hand, citizen users may use Graphical User Interfaces to compose and configure software to solve the configured tasks. However, those GUI tools, most commonly portals running on web servers, in turn re-use the APIs and interfaces that are available to the expert users within the same domain.

However, both citizen and experienced users are served by an organisational structure providing and establishing an end-to-end service for all of its users by leveraging and integrating platforms and platform services made available by the appropriate experts.

5 Federated Virtualised Infrastructure

As indicated in the scenarios described in section 3 a set of core services must be deployed within and across EGI's resource providers. Wherever possible, the services are described by functionality and applicable standardised interfaces. This ensures the resource provider's freedom of choice as to which concrete software they deploy to expose their respective core service, leveraging any existing expertise in particular software stacks and management infrastructure already present. Services that cannot be described using existing standards, specific software stacks are described that must be deployed to deliver the respective service. It is expected that these will evolve into standardised service interfaces over time.

From the scenarios described above a set of core services must be present. The following figure shows on a conceptual level the arrangement and facing of the described services.

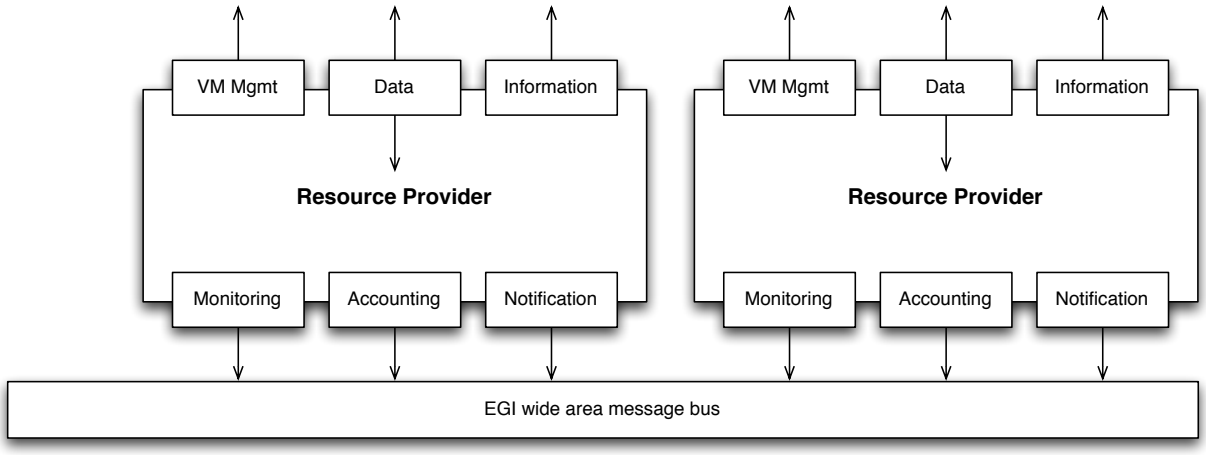

Figure 2: Core services deployed by and used at their federated resource providers

Together, these core services comprise the EGI Cloud profile as described in more detail in the next section.

5.1 Deploying EGI Cloud services

The previous sections identified several core services and interfaces that must be supported by the EGI resource providers. However, nothing was said about how these services are deployed, or who 'owns' those services and therefore governs their use, publicity and scope.

Figure 3 gives an indication of how these service should be deployed, and with which scope:

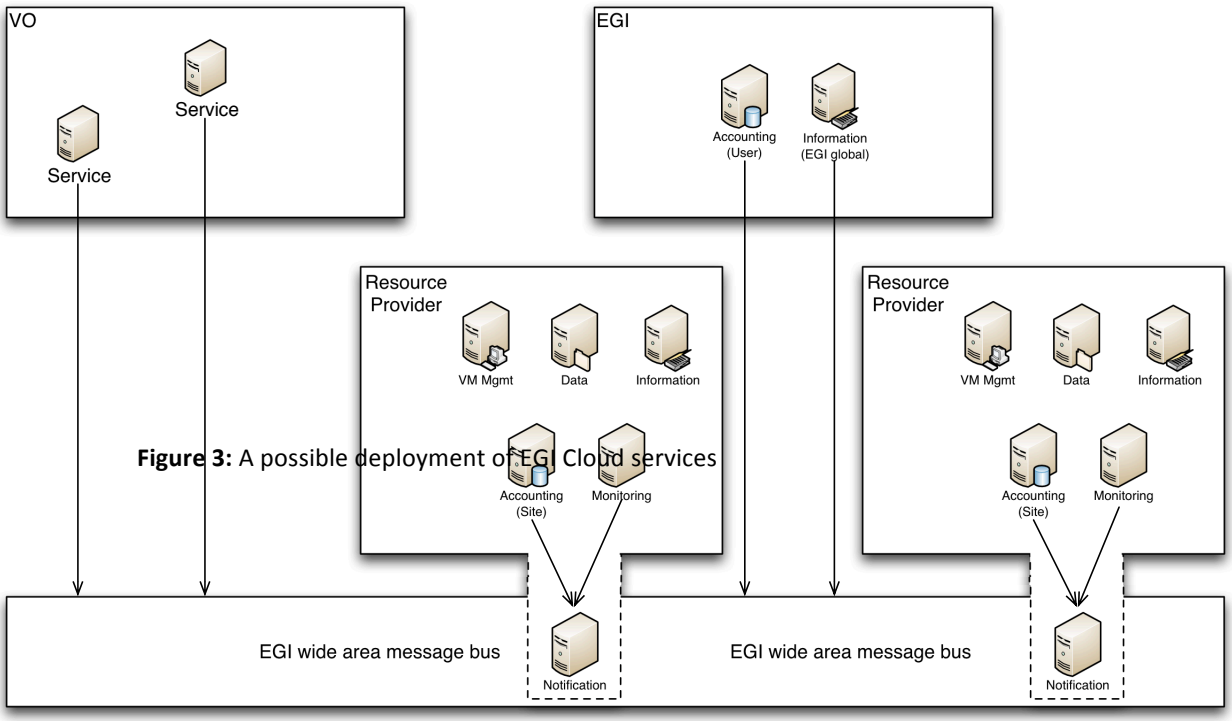

Figure 3: A possible deployment of EGI Cloud services

The EGI message bus is not a centrally managed but physically distributed "network of brokers" that operates on a store/forward fashion for the management of the operational infrastructure, providing the messaging clients (producers as well as consumers) a consistent distributed messaging fabric irrespective of the actual location of the client. As indicated the brokers are located within a resource provider hence within the governance of the respective provider, but exposed into the network of providers to build the messaging fabric across all resource providers. While the store/forward pattern is used to provide scalability, it may be combined with resource provider-local master/slave configurations to ensure high availability of the service.

Centralised EGI services (comparable to the current EGi Global Tasks) may access the message bus, for example providing a globalised service description service, or an accounting portal for user orientated accounting services. Although illustrated as under the domain of EGI, those centralised services do not necessarily have to be run within the EGI domain, or on EGI resources – those services are easy to delegate, perhaps using the virtualised resources themselves.

Figure 3 also illustrates VO services accessing the federated EGI messaging infrastructure. As described earlier in this document, this use case highly depends on the effective model EGI's VOs adopt in exploiting the virtualised infrastructure.

In this context, one may claim that one characteristic of Cloud computing is not, or only partially met. *Resource pooling* as defined by NIST [R 1] commonly implies a certain degree of location independence. In the presented model, this is certainly true at the level of resource providers federated into EGI. *Within* resource providers, each resource provider ensures local location independence as an implementation detail through the VM Management service interface exposed. Across resource providers however, the presented model facilitates location independence by insinuating only indirect access to the virtualised infrastructure through VOs providing SaaS offerings to its end users.

6 EGI Cloud Profile

The EGI Cloud Profile defines the technical and functional interfaces for the core services each resource provider must provide or implement to be considered for inclusion into EGI.

6.1 EGI Cloud Services Profile

The following sections describe the services in greater detail.

6.1.1 Infrastructure messaging

Deployed ActiveMQ.

6.1.2 Monitoring

Deployed Nagios. New probes needed.

6.1.3 Accounting

Deployed accounting repository and portal. Work is underway to make changes to support virtualised resources.

6.1.4 Notification

6.1.5 VM Management

OCCI supported on the deployed.

6.1.6 Data services

GridFTP, SRM, CDMI

6.1.7 Information services

Deployed BDII. New information providers needed.

6.1.8 Authorisation

Existing VOMS.

6.1.9 VM Repository

Reuse existing prototypes from CERN?

7 Glossary

The following glossary explains terms used, and partially introduced, throughout this document.

Resource Provider	A Resource Provider is an entity offering compute or storage capacity, or both, in its cloud for users to consume.
VEE	**V**M **E**xecution **E**nvironment
VM	**V**irtual **M**achine
VMM	**V**irtual **M**achine **M**anagement
VO	**V**irtual **O**rganisation

8 References

R 1 NIST Definition of Cloud Computing, http://csrc.nist.gov/groups/SNS/cloud-computing/

R 2

R 3

R 4

R 5