Communications Networks, Content and Technology
European Commission Directorate General

European Union's Horizon 2020 Programme
European Commission
Directorate General for Communications Networks, Content and Technology
eInfrastructure

Magic
Middleware for collaborative Applications and Global vIrtual Communities

Deliverable D3.6

Recommendation on service requirements for cloud providers in academic cloud infrastructures

This project is co-funded by the Horizon 2020 Framework Programme of the European Union

A project implemented by RedCLARA

Progress Report

MAGIC Deliverable: D3.6 Recommendation on service requirements for cloud providers in academic cloud infrastructures.

Document Full Name	**MAGIC WP3 D3.6 Recommendation on service requirements for cloud providers in academic cloud infrastructures.**
Date	**6-2-2017**
Activity	**Cloud Provisioning and Groupware Standards**
Lead Partner	**CLARA**
Document status	**Final**
Classification Attribute	**Public**
Document link	

Abstract: This document with recommendations regarding cloud service parameters is envisaged as a reference for organizations that are interested to provide cloud services in a global academic environment. The goal is that institutions can define their service parameters so as to provide services according to a set of common standards..

COPYRIGHT NOTICE

MAGIC (Middleware for collaborative Applications and Global virtual Communities – Project number: 654225) is a project co-funded by the European Commission within the Horizon 2020 Programme (H2020), Directorate General for Communications Networks, Content and Technology - eInfrastructure. MAGIC began on 1st May 2015 and will run for 24 months.

For more information on MAGIC, its partners and contributors please see http://www.magic-project.eu.

DELIVERABLE ROUTE

	Name	Member/Activity	Date	Responsible
From	Gustavo A. Garcia	Technical Manager	2017-2-15	RedCLARA
Contribution by	Fernando Aranda	CUDI	2017-2-27	CUDI
Contribution by	Michal Procházka	CESNET	2017-2-28	CESNET
Contribution by	Christos Kanellopoulos, Ognjen Prnjat	GRNET	2017-3-30	GRNET
Contribution by	Carlos A. González P.	Development Project Leader	2017-3-20	RedCLARA
Approved	Florencio I. Utreras	Project Coordinator	2017-04-05	RedCLARA

TABLE OF CONTENTS

This project is co-funded by the Horizon 2020 Framework Programme of the European Union

A project implemented by RedCLARA

1. INTRODUCTION

It is in the interest of National Research and Education Networks (NREN), R&E infrastructure providers and data centres, and institutions like universities, colleges and research centers to share services with each other for the benefit of their users and for economies of scale. The cloud technologies available provide multiple advantages like service sharing, stability, activation speed, and reliability among many others, due to the concept of concentrating services on dedicated providers and data-centers. With this rich environment of services and infrastructure, other challenges appear like evaluating and contracting the most capable providers, ensuring security and data privacy. This recommendation aims to provide a reference for the client institutions to asses service providers' capabilities, and request the service parameters that suit them. . This reference does not intent to be a contract, but to serve as a guideline for the relevant requirements. The providers can thus specify the relevant parameters of their service provisioning profile, while the consumer can define what requirements fulfill their needs. . A cloud provider could be and academic institution or commercial entity. In both cases, the contracting party / consumer will act as an intermediary to represent their organization and users interests, based on their own service standards.

As such, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this section are to be interpreted as described in RFC 2119[1].

2. GLOSSARY

AUP: Acceptable Use Policy
CSP: Cloud Service Provider
NREN: National Research and Education Network
REN: Research and Education Network
SAML: Security Assertion Mark-up Language
SLA: Service Level Agreement

[1] http://tools.ietf.org/html/rfc2119

3. SERVICES DESCRIPTION

This section describes the kind of services that are part of these requirements.

Infrastructure as a Service (IaaS): Services that provides resources to support end-user service deployment. In this area are included services like connectivity, cloud servers, authentication infrastructures, data storage, among others.

Software as a Service (SaaS)/Cloud Application Services: Software services for institutions or end users, which are offered by cloud providers for a specific purpose. Examples of these services include e-learning systems, email-severs, office365, among many others.

Platform as a Service (PaaS):
Services that are in the cloud and provide tools and resources to develop, test, manage and deploy applications and systems.
In this model end users can become providers or users of a service.
Examples are database management systems, design tools, operating systems, and many others.

Services catalogue: Service that list and describe the existing services, applications, infrastructures including its characteristics, policies, and attributes.

Federated access: Defined as the support for the federation protocols stack in order to allow the end-users to access services in other domains, by using its home institution credentials for authentication.

Service data/end-user data: Any information generated or stored in any format by the institutions, end-users, communities, or stakeholders. It also include all the information generated from their use, combination or modification.

4. THE RESEARCH AND EDUCATION ORGANIZATIONS AND SERVICE ROLES

National research and education networks are typically non-profit organizations , whose purpose is to provide connectivity for research and educational institutions and to support the educational, innovation and research activities by providing various value-added applications and services to its customers, on top of basic connectivity.. Examples of such applications can be basic collaborative applications such as videoconferencing, file transfer, etc, through provisioning of IaaS services such as data storage, on-demand cloud Virtual Machines (VMs), supercomputing facilities, via digital libraries, all the way to discipline-specific applications in diverse fields such as climatology, astronomy, biomedicine, etc.

5. ACCESS TO THE NETWORK

NRENs and academic institutions rely on its academic networks for ensuring the quality, privacy, security and performance of its services. Due to this, it is required that the cloud providers are connected to the an NREN or REN in order to provide services to the community.

6. COMPLIANCE WITH IDENTITY FEDERATION STANDARDS

a) The provider must support the SAML protocol in a recent version, and be capable to behave as a service provider according to the SAML specification.

b) In order to support access for users from academic institutions around the globe, the provider should be part of the national identity federation which is connected to the inter-federation eduGAIN.

c) It is desirable but not mandatory that the provider has the ability to implement an interface for group management in federations based on a standardized protocol like VOOT, SCIM or SAML2 Attribute Query. The group management functions aims to work for authorization or perform functions based on group members or membership which are not available from the user's home organization. Group membership is usually managed by the research projects and communities.

7. ORGANIZATION REQUIREMENTS

The provider must declare, and ensure its organization adheres to the following:

a) Shall not be under investigation for any corruption or illegal activity, including money laundry.
b) The organization must not be in bankruptcy protection laws
c) The related services shall not be under dispute, or legal copyright processes. Furthermore, all the offered services must be of its property or have an agreement for commercial use.

8. PRIVACY AND USE OF DATA REQUIREMENTS

a) IPR in respect of customer data

The provider shall not use any of the user's data for any purpose, not related to the service delivered.

The provider shall respect the original copyright of the customers' data. The above means that the use of any of the provider services will not transfer data ownership, even if this is notified, suggested or accepted by the end-user during the service use.

b) Processing data

For any processing of the end-user data an agreement is required with the client institution, or owner of the data.

c) Ownership of the data

All service data will be owned by the end-user and the institution she/he belongs too.

The end-user shall always have guaranteed access to this data. The provider shall guarantee that the user will have the possibility to access hers/his information, independent of the current service status. In case the end-user does not have the active services with the provider, she/he will have the right to request a backup copy of hers/his last information.

d) Data protection

The CSP should treat all User data as though it were confidential regardless of its classification by the User. It is anticipated that CSPs will be required to evidence that they will cascade this responsibility down its supply chain to all relevant 3rd parties. It is also anticipated that User will expect CSPs to make every effort to safeguard data access and the interests of the Users at all times. CSPs will be expected to ensure that all staff sign a confidentiality statement regarding confidential data.

e) Request data access from 3rd parties

Where a request for access to User data comes from a recognised government authority, the CSP will be expected to check what their actual legal obligation is before they comply with the request. Users do not expect the CSP to cooperate where no legal obligation exists and thus deny the request. Where a legitimate request is received, the CSP should only release a minimum data set and in all cases will be expected to inform the affected User as soon as possible.

f) Notification

The CSP should notify the User immediately if it becomes aware of a suspected or actual breach of confidentiality, loss of data, breach of the security measures, deterioration of the service, or downtime of the service. The CSP will take all necessary measures, at its own cost, to secure the data and to rectify the shortcomings in the security measures so as to prevent any further perusal, alteration, or provision, without prejudice to any right of the User to damages or other measures. Following such an incident, at the User's reasonable request, the CSP will cooperate with the provision of information about the incident and its resolution to concerned parties.

g) Data location

The CSP must provide, if requested by the institution, the location of their servers and its cloud infrastructure related to the offered services. The above includes the facilities where information is stored, processed or transit.

9. ACCEPTABLE USE POLICY (AUP)

The provider should have an acceptable use policy that describes what it considers an improper or outright illegal for the use of its service. This AUP must be properly communicated to end-users before they use the service.

10. DATA PRESERVATION AND ACCESABILITY

a) The provider shall make all efforts and have strategies for keeping customers' data safe. The above means it shall have periodic backups, restore tests, disaster recovery plans, and high redundancy levels. The strategies for data preservation must be described.

b) The provider shall guarantee the end-user is able to access her/his data in the presence of any event including, but not limited to: charging/credit disputes, service suspension, service cancellation, user migration to other provider or service. The provider must give the mechanism to download, backup, or carry out snapshots for the mentioned purpose.

11. SERVICE CHARGING AND USAGE

The provider must ensure the customer charging model be predictable and clear for the end-user. In order to do so, the provider must:

a) To provide clear and accessible channels to request service changes, and cancellations, ensuring always customer agreement with their bills.

b) Describe all fixed and variable rates applicable for the service

c) Provide thresholds that avoid high rates that could impact customers budget

d) When possible, provide projections of the estimated maximum expenses.

e) The provider must provide a mechanism for the users to claim a credit reimbursement in case of outages

12. SERVICE LEVEL AGREEMENT AND QUALITY REQUIREMENTS

a) The provider shall have a well defined Service Level Agreement (SLA) in where the provider specifies: I) The service availability, II) If there is any compensation for no compliance, III) The support scheme, IV) Metrics available and V) the escalation procedures.

b) It is highly recommended, that the above SLA commitment includes a high service availability agreement.A high service availability can be considered above 99,5% monthly.

c) The provider must specify the service desk structure, attention channels, languages supported, and service hours.

d) The provider must have a change management process that guarantee users' notification of maintenance activities.

e) The provider must have performance and usage monitoring capabilities, and the resulting information shall be available to the academic institutions.

13. MANAGEMENT ROLES

The service provider shall designate the following roles, and provide all its contact information:

a) **Service manager:** In some cases, this role can be divided in a service delivery manager, and a service manager. The responsibilities of this/these roles include: i) Guarantee the delivery of services in time and quality, ii) Foster high quality and the compliance of service level agreements, iii) Be the customer representative inside the provider's organization.

b) **Technical contact**: A person or area in command of attending any engineering, dimensioning or technical requests that my arise. This area is the first escalation contact for technical inquiries.

14. SERVICE REQUIREMENTS

a) The infrastructure services provider must have a detailed service description of their technologies. Including:
   i. Virtualization technology used
   i. Technical standards supported
   ii. Compliance with international norms and standards

b) The service provider must have the ability to provision resources quickly, easily and efficiently.

c) The service provider must have a detailed service backups.

d) The service provider shall guarantee that the end-user and the institutions will be able to transfer their services to other infrastructures. This process shall be done by using standard formats, in a practical and usable form.

15. SOFTWARE SERVICE REQUIREMENTS

a) Is desirable that the offered solutions are open-source.

b) The provider must guarantee that its service does not brake any intellectual property laws for the users' access or utilization. In case of using commercial software, the provider shall specify the licensing costs, and how are they related to service charges.

16. COLABORATORIO'S INTEGRATION REQUIREMENTS

In this project, we have enhanced a global platform intended to facilitate the integration of services and provide them to end user communities, this platform is called the Colaboratorio. Today Colaboratorio provides its integrated services to end-users and institutions in Latin-America, Europe, Africa, the Caribbean, Middle-east and Asia.

The Colaboratorio platform includes today applications developed by NRENs and RRENs in Europe and Latin America, such as: VCExpresso for web-videoconferencing, FileSender for large files transfer, Docs for collaborative document construction, and several other. These applications make use of a

Single Sign-on service and adopt the user-group standards promoted by this project. In this section we develop a series of recommendations for other developers to ensure that their applications can be inserted in this platform. The applications can then be provided as stand alone or in the cloud by NRENs, RENs, or commercial providers taking into account the following requirements:

a) Providers must comply with SAML identity federation standards declared in numeral 6.

b) Colaboratorio has a mailing list management service in their suite. This service is usually based on mailman, and there is an integration with the Sympa server too. In case of deploying their own mailing-list management, the provider must implement an API that supports the following commands:
   a) createList(_list_name_, _list_owner_) /*creates a new list*/
   b) listMembers(_@members_) /*updates the members of a list*/
   c) getMessages(_date_) /*returns the messages received from _date_*/

c) Colaboratorio's communities management service is deployed through Iframes integration. In order to support it, the provider's application must allow to be embed in HTML Iframes.

d) The provider shall allow to share meta-data with Shibboleth base identity providers. The above will allow to be integrated to the confederation service called eduGAIN.

e) The service to be integrated must be encrypted through SSL. For it, the service must implement a valid SSL certificate.

f) The provider must accept the Identity Providers' meta-data shared by RedCLARA's service. In other words, the providers shall allow service login from RedCLARA's partners, including the European confederation eduGAIN.

g) The service should be capable of reading a language string via URL, for example lang=pt, l=pt, /pt/ or similar.

h) It is recommended that the service become adapted to the Colaboratorio's look and feel following these minimum guidelines:
   a) Using bootstrap Stylesheets
   b) Avoiding any menu to the left.
   c) Avoiding any header.

d) Avoiding any log out button.
e) Using “Open Sans - 12px” as body text.
f) Using “Open Sans - 22px” for Level 1 titles.
g) Using “Open Sans - 18px” for Level 2 titles.

17. SECURITY REQUIREMENTS

The service provider shall be able to deliver the following information to the institutions, so they can asset the overall security status:

a) The cloud service provider must have their infrastructure in a secure location, protected in physical access with a strict control procedure, network access through firewalls and intrusion detection systems, and policies that defines the minimum security standards adopted.

b) The provider should have a framework for information security management - Example ISO27001 - 27002

c) Provider must have periodic security audits that help to prevent security incidents. The minimum recommended period is 1 year.

d) It is recommended that the provider has a Security area and/or Computer Security Incident Response Team (CSIRT), in command of attending security incidents and defining preventive measures. In addition, the provider must describe its procedures for managing security incidents,

e) Provider should have a secure data deletion procedure

f) Provider should have a disaster recovery plan to ensure continuity. The plan shall include infrastructure and application recovery.

18. REFERENCES

[1] Mandeep Saini (GÉANT), GN42-16-114E4 GÉANT IaaS Cookbook

[2] Cloud Standards Consumer Council (CSCC), April 2015, Practical Guide to Cloud Service Agreements Version 2.0