Computer Standards & Interfaces 47 (2016) 19–23

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Standards for enabling heterogeneous IaaS cloud federations

Álvaro López García*, Enol Fernández del Castillo, Pablo Orviz Fernández

Institute of Physics of Cantabria, Spanish National Research Council — IFCA (CSIC—UC), Avda. los Castros s/n,39005 Santander, Spain

ARTICLE INFO

Article history:
Received 23 November 2015
Received in revised form 28 January 2016
Accepted 2 February 2016
Available online 15 February 2016

Keywords:
Cloud computing
Standards
Interoperability
Federation

ABSTRACT

Technology market is continuing a rapid growth phase where different resource providers and Cloud Management Frameworks are positioning to provide *ad-hoc* solutions–as management interfaces, information discovery or billing–trying to differentiate from competitors resulting in incompatibilites between them when addressing more complex scenarios like federated clouds.

Therefore, grasping interoperability problems present in current infrastructures by studying how existing and emerging standards could enhance the cloud user experience.

In this paper we will review the current open challenges in Infrastructure as a Service cloud interoperability and federation, as well as point to the potential standards that should alleviate these problems.

1. Introduction

Cloud computing is still considered as an emerging technology, now leaving its infancy phase. Standardization in the cloud was not considered as an urgent topic by the industry [1], as it is often associated to rigidity, not leaving much room for the innovation needed on the early stages of the technology [2].

Over the last years, a large number of commercial cloud providers have emerged in the market. Each of those vendors tries to differentiate their infrastructure from their competitors offering added value features on their resources. This has led to a situation where several closed and proprietary interfaces have evolved over the time, some being claimed as *de-facto* standards by the industry, even if they cannot be considered a proper standard at all. The resulting scenario is formed by infrastructures using different solutions that are incompatible and not interoperable, constricting users inside a single provider. These vendor lock-ins are often considered a desirable feature by commercial providers, as a way of engaging users on their resources and services, but it is perceived negatively by cloud users and customers [3].

More recently, several open source Cloud Management Frameworks (CMFs) have appeared in the cloud ecosystem. Some of them decided to adopt the most popular commercial and proprietary interface, implement a compatibility layer that tries to deliver the same functionality; whereas others have built their own interface. Both decisions are contributing to adding more entropy and heterogeneity into the cloud ecosystem. Users willing to exploit several infrastructures face a discouraging panorama, with strong industrial actors driving the developments that have promoted a situation where proprietary and industry-driven interfaces and protocols have dominated the cloud landscape for years [4].

As the cloud computing paradigm is maturing and its heterogeneity is growing, cloud interoperability and federation are becoming areas of concern [5,6]. Federation and interoperability are nowadays considered as one of the main pressing issues towards cloud computing adoption [7]. The vendor lock-ins that currently exist are perceived negatively by users, therefore building and defining frameworks for cloud interoperability is becoming a topic with growing interest [8,9,10,11,12,13]. Moreover, political and government bodies such as the European Commission have stated their position towards the promotion of Open Standards for ensuring interoperability in clouds for science and public administration [14,15].

Nevertheless, cloud federation goes beyond just making several clouds interoperable [16]. A federation should enable the collaboration and cooperation of different providers, delivering resources to the users when a single resource provider is not able to satisfy the user demands, in a collaborative way. Therefore, on top of the interoperability and portability issues, there are several challenges that any federation must tackle.

In this paper we will review the open challenges when building an interoperable cloud federation. We will review the existing enabling standards that can be used to leverage the construction of such a federation of Infrastructure as a Service (IaaS) providers based

* Corresponding author.
E-mail addresses: aloga@ifca.unican.es (López García), enolfc@ifca.unican.es (E. Fernández del Castillo), orviz@ifca.unican.es (P. Orviz Fernández).

http://dx.doi.org/10.1016/j.csi.2016.02.002
0920-5489/

on them. We will focus on a *horizontal federation* between different IaaS providers, Therefore a *vertical federation* spanning several layers is out of the scope of this paper.

In Section 2 we will present the related work in the area. In Section 3 we will present the biggest challenges that an interoperable cloud federation must assess. In Section 4 we focus on the existing and raising standards and how they can be used to tackle the problems presented in Section 3. Finally we present our conclusions in Section 5.

2. Related work

Some work and research have been done into cloud interoperability, although a lot of the work is regarding cloud *portability* between different cloud infrastructures.

There are many non academic works regarding the need, or lack thereof, for a *cloud standard*. However, authors agree that there would not exist such a unique standard to rule all the cloud aspects. Some preliminary work regarding the need of standards for the cloud has been done in the past [3,17].

The United States National Institute of Standards and Technology (NIST) has surveyed the existing standards for interoperability, performance, portability, security and accessibility in the Cloud Computing Standards Roadmap [18]. However, there are some aspects like information discovery or accounting that are missing in this study.

The G. Lewis [19] report tackles several standardization areas such as workload management, data and cloud management APIs, concluding that there will be not a single standard for the cloud due to pressures and the influences of existing vendors. The author states that an agreement on a set of standards for each of the needed areas would reduce the migration efforts and enable the third generation of cloud systems.

Harsh et al. [20] work surveyed the existing standards for the management of cloud computing services and infrastructure within the Contrail project so as to avoid vendor lock-in issues and ensure interoperability. In the same line, Zhang et al. [21] carried out a complete survey regarding Infrastructure as a Service access, management and interoperability, studying OVF, CDMI and OCCI. However, the analysis lacks other federation challenges.

On top of those academic efforts, some open source Cloud Management Frameworks (CMFs) have started to take into consideration the federation issues. There are development efforts aimed to make possible to federate different aspects of distributed cloud infrastructures to an extent:

- OpenStack [22] implements several levels of federation by the usage of cells and regions. Cells allow to run a distributed cloud sharing the same API endpoint, whereas regions are based on having separate API endpoints, federating some common services. On top of that, OpenStack also implements a federated authentication mechanism [23], making possible to authenticate users coming from trusted external services or third-party identity providers.
- CloudStack [24] follows the same line as OpenStack and implements the concept of regions in their software.
- OpenNebula [25] makes possible to configure several installations into a tightly integrated federation, sharing the same users, groups and configurations along several cloud sites.
- Eucalyptus [26] provides identity federation, making possible to reuse the same credentials in several Eucalyptus infrastructures.

However, all of these solutions are focused on federating several instances of the same CMF (i.e. several OpenNebula installations, for instance), being impossible or difficult to federate disparate and heterogeneous infrastructures (e.g. an OpenStack installation together with an OpenNebula instance).

There a few prominent existing federated infrastructures, some of them being built on top of standards. Some examples of standards-based federations are the EUBrazil Cloud Connect [27], whose middleware is being based on standards for interoperability [28]; and the European Grid Infrastructure (EGI) [29], that started as a federation of grid sites, took the strategic position of exploring and adopting a technology agnostic and based on open standards cloud [12] into their services portfolio. In this context, the Open Science Cloud initiative [30] has outlined that interoperable, distributed and open principles should drive the evolution of Science Clouds as the key to success.

3. Cloud federation open challenges

As we briefly exposed in Section 1, a cloud federation should take into account other aspects apart from interoperability and portability such as authentication, authorization or accounting. In the following sections we will elaborate on the open challenges regarding cloud federation.

3.1. On uniform access and management

One of the first obstacles that a heterogeneous cloud federation has to overcome is the lack of a unified cloud interface. Evolving from commercial cloud providers, each middleware implements their own — proprietary or not — interface. Some open CMFs implement an Amazon Web Services (AWS) EC2 [31] compatibility layer, since it was considered as the most popular commercial interface for the cloud.

The adoption of the AWS EC2 API could make two different CMFs being interoperable, but it presents several obvious drawbacks. First of all, its usage and promotion introduce a vendor lock-in, as users can be locked into one infrastructure if the original vendor decides to change its API from one day to another. A proprietary API is subject to change without prior advice by the original vendor. This will render into incompatibilities between providers and CMFs other than the original creator of the API, Amazon in this case. Implementers of such proprietary interfaces need to keep aligned with the reference implementation, and are forced to invest time in following the modifications so that they ensure that its implementation remains compatible.

Secondly, the EC2 Query API is not RESTful [32]. Even if it uses the standard components of the HTTP protocol to represent API actions it does not use the HTTP message components to indicate the API operations, being them expressed as parameters (in the URI parameters of a GET request or in the body of a POST request). This URI-based parameter passing is not enough for defining an interoperable API allowing a standardized implementation. Moreover, as it is not RESTful, it introduces additional complexity for developers exploiting these clouds, as they have to learn the semantics being used instead of the well known REST architectural style. Lastly, the usage of the query component of an URI to obtain hierarchical data goes against the RFC-3986 “Uniform Resource Identifier (URI): Generic Syntax”[33], as it states that “The query component contains non-hierarchical data that along with data in the path component, serves to identify a resource (…)”.

3.2. On portability

Cloud computing leverages virtualization technologies to abstract the resources being offered to the users. Several virtualization hypervisors (such as Xen, KVM, VMWare, Hyper-V) exist in the market, and each cloud provider uses the one of its choice (or even a combination