THE IETF SHOULD CREATE AN INTERCLOUD RFC
The Interfaces In The IETF Cloud Reference Framework Should Be Standardized

Jan Sipke van der Veen
TNO, Groningen, The Netherlands
jan_sipke.vanderveen@tno.nl

Robert J. Meijer
University of Amsterdam, Amsterdam, The Netherlands
rmeijer@science.uva.nl

Keywords: Cloud Computing, Standardization.

Abstract: This paper discusses the current state of cloud computing and shows that it is comparable to the state of networks before the internet. Clouds need to be connected more to make it easier for users to switch between providers and at the same time make it easier for providers to supply ”infinite resources”. At the moment the big cloud providers do not feel the need to standardize this intercloud and there is no authorative body that sets the standard. This paper argues that it is necessary for the IETF to take its current effort to create a cloud reference framework one step further and standardize the interfaces between the functions and layers as well.

1 INTRODUCTION

The concept of computing as a utility has been around since the 1960's (Parkhill, 1966), but it took until the mid 2000's for cloud computing to turn that concept into a reality. The past years have shown a rapid uptake in its usage and a lot of providers have joined the market (Armbrust et al., 2010). Although their services are similar in concept, the differences between them make it difficult for users to switch from one provider to another. We argue that standardization of a reference framework alone is not enough to realize the intercloud. The interfaces between cloud functions and layers should be standardized as well.

This paper will discuss the currently disconnected clouds in section 2, describe the potential of the intercloud in section 3 and make the case for the need of standardization of the intercloud by the IETF in section 4. Finally it presents two cases where standardization of the intercloud would be very beneficial in section 5.

2 DISCONNECTED CLOUDS

Cloud computing is still a relatively young phenomenon. Amazon played a key role in the development of cloud computing when it launched Amazon Web Services (AWS) and specifically Elastic Compute Cloud (EC2). Several providers followed in the next years to offer network based IT services in a pay per use fashion. These services can be grouped into one of three service models (Mell and Grance, 2009): Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Because of technical differences between these offerings it is hard to switch from one provider to another. This is true even for similar services within the same service model. For example, transferring an e-mail archive from one provider to the next is impossible if not all providers allow a protocol like IMAP to extract all current messages from the system.

Cloud computing is often attributed ”infinite resources”, at least in the eyes of the consumer. However, this apparent infinity of resources comes at a price to the provider. He must ensure that enough resources are available when demand increases unexpectedly. A relatively high percentage of resources is therefore unused most of the time in small clouds. In bigger clouds this percentage can be lower, but is still limited by the size of a single cloud.

The state of cloud computing looks a lot like the state of networks before the internet. Networks used to be disconnected and connectivity between networks could only be achieved with networks of the same type. Internet changed all this by defining layers

on top of the disconnected networks, see left side of figure 1. Even though the separate networks still use different technologies, e.g. ethernet and roken ring, the layers on top ensure that communication between them is possible.

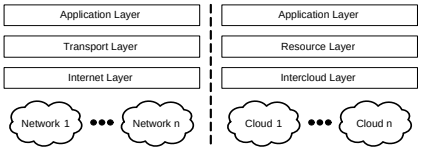

Figure 1: Current internet RFC (left) and possible intercloud RFC (right).

3 CONNECTED CLOUDS

The tranformation of all these separate clouds into a connected intercloud would bring great benefits to its users as well as its providers.

The most important benefit for users would be the ease of switching between providers. Taking the example of the internet again, it is currently easy to switch from one network vendor to the next. It does not even matter if the network is provided via a fixed line, a mobile connection or via satellite, each and every machine using IP can communicate with all other machines using IP.

The intercloud would benefit providers as well. It allows them to share their resources in such a way that the percentage of unused resources, waiting for unexpected demand, can be much lower per provider. Currently, a provider attracting mostly UK customers probably needs more resources during UK office hours. To meet this demand, a lot of resources are unused during the night. In the intercloud scenario, a provider with mainly US or Australian customers could use these resources during their office hours.

At the moment the big cloud computing providers do not feel the need for standardization. They mainly see the drawbacks of a standard which allows customers an easier move to their competitors. The smaller providers and especially the users would like to see such a standard, but the current efforts in this direction are not good enough. The (proposed) standards are either limited in scope or the authors are not seen as authorative. In our opinion the IETF would make the ideal candidate to describe such an important cloud standard. The right side of figure 1 shows how such an intercloud RFC may look quite similar to the existing internet RFC.

4 STANDARDIZATION

Standardization of cloud computing would need to address several aspects of cloud technology, but also some business cooperation between its providers.

4.1 Interoperability

One of the first areas of standardization should be the interoperability between different clouds. We will distinguish between the three service models again, because they differ very much in the level and type of standardization that can take place.

4.1.1 Software as a Service

Standardization in this service model should address the input and output format(s) of the user data, e.g. how the messages in an e-mail service should look like. It should also define the protocol(s) for transmission of this data, e.g. which steps are necessary to transfer the messages out of the e-mail service. In the general case this is hard to achieve, because there are so many different (possible) services. But for specific types of services it is quite possible to define certain requirements on these formats and protocols. Several standards are therefore needed in this service model, one for each service type.

4.1.2 Platform as a Service

Standardization in this service model should address the programming APIs. Ideally, this standard would be language independent or at least easy to use in different languages. Of course there will always be a need for providers to distinguish themselves from their competitors. This can be achieved by providing a common set of calls that are mandatory and a set of optional or extendable calls that should be clearly marked as such. This leaves the user free to choose between interoperability and extra functionality that is specific to a certain provider. In this case providers can still make their own decisions about the programmaging languages they offer. But if they do offer a specific one, the user can be sure that his application, using only mandatory calls or supported optional calls, will work with this provider.

4.1.3 Infrastructure as a Service

Standardization in this service model should address the virtual machine representation. One part of this is the representation of the state of the virtual machine, e.g. the harddisk and the memory contents of a paused virtual machine. Another part is the representation of

metadata about the virtual machine, e.g. the amount of memory and the number and type of processors it contains. Standardization should also address the interaction with the virtual machines from a client computer. This interaction, also with the cloud as a whole, is especially important for management tools. To be able to make informed decisions on the number of acquired virtual machines and their providers, it is also necessary to standardize the cost reporting of the different virtual machines at offer.

4.2 Federation

A second area of standardization should be the federation between different clouds.

4.2.1 Identity and Security

To create the illusion of a single cloud to its users, there is the need for a shared sense of ”who is who”. This can be achieved by standardizing on a federated identity management method. Currently authentication is mostly achieved with preshared passwords, but can also be more secure with public and private keys. It is vital for the intercloud to have a common set of authentication methods, perhaps with restrictions on the capabilities if a less secure form of authentication is used.

Creating a secure connection between servers in the cloud and servers located elsewhere is a big issue. This issue needs to be resolved for the intercloud to work properly, because it depends on a much more fluid landscape of servers that need to communicate in a secure fashion.

4.2.2 Accounting and Billing

In the intercloud scenario it would make sense for a user to subscribe to a single cloud and be able to use resources of other clouds without being aware of the technical and business differences between these clouds. Much in line with a need for a federated identity management method therefore is the need for federated accounting and billing methods. This would allow the cloud providers a way to keep track of the billable activities of the user, even if these activities take place in other clouds.

4.3 IETF

The IETF is currently working on or has worked on several draft standards involving cloud computing:

- A6: The Automated Audit, Assertion, Assessment and Assurance API (Hoff et al., 2010)
- LISP: Locator / Identifier Separation Protocol (Farinacci et al., 2009)

These two draft standards focus on specific parts of cloud computing. The first draft standard provides an open, extensible and secure interface that allows cloud computing providers to expose audit, assertion, assessment and assurance information for IaaS, PaaS and SaaS services. A client would then be able to interrogate the service and verify compliance with local policy before making use of it, e.g. by checking the geographical location of the servers. The second draft standard describes a simple, incremental, network-based protocol to implement separation of internet addresses into endpoint identifiers and routing locators. This would alleviate some of the scaling issues currently visible in network routing.

The IETF is also currently working on reference frameworks that can be used to guide the standardization of cloud computing:

- CSF: Cloud Security Framework (Karavettil et al., 2010)
- CRF: Cloud Reference Framework (Khasnabish et al., 2010)

The first one deals with the security aspects of cloud computing and establishes security standards, policies, procedures and guidelines for cloud providers. This framework would enable cloud providers and cloud users to practice safe security techniques for their applications and intracloud and intercloud information exchange. The second framework addresses cloud computing in a more general way. This Cloud Reference Framework involves basic functions or layers to support the general requirements of cloud applications and services. It divides itself into four horizontal layers and one stacked vertical layer to support configuration management, registry, logging and auditing, security management and service level agreement (SLA) management, see figure 2.

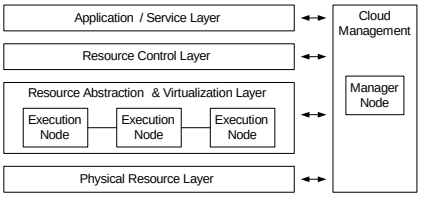

Figure 2: Cloud Reference Framework (draft).

The Cloud Reference Framework seems very promising as it provides a common understanding of the different cloud computing functions and layers. In our opinion it should form the basis for another standard that describes the interfaces between the functions and layers described in the framework.

5 CASES

This section discusses two cases where standardization of the intercloud would be very beneficial.

5.1 Early Warning Systems

Early Warning Systems (EWS) provide a technological alternative to human survaillance on critical infrastructures like dikes and bridges. These systems take sensor data from the monitored infrastructure, analyse the data and report to other information systems or people about the state of the infrastructure, see figure 3.

During normal operation of an EWS, i.e. there is nothing wrong with the infrastructure, not much computing capacity is needed to run the analysis. However, if things are about to go wrong, e.g. the EWS thinks a dike section will break soon, a lot more computing capacity is needed. This capacity is needed for instance to simulate the water flowing through the dike section and into the urban area behind it.

An EWS is therefore a very good candidate for cloud computing. It would be very inefficient to have this much computing capacity standing by just in case something goes wrong with the monitored infrastructure. However, there is a risk in using a single cloud provider for such an important IT system as an EWS, which may warrant the extra cost involved in setting up dedicated computing capacity. The intercloud would solve this dilemma, because it allows for very fast switching of providers if something goes wrong with one of them.

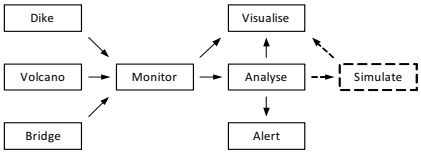

Figure 3: Early Warning System (EWS).

5.2 Dynamic CDNs

Content Delivery Networks (CDN) are widely used to distribute content to users. In a CDN, content is distributed to several nodes owned by the CDN operator. If a user requests this content, he is redirected to a node that is able to provide the content in a fast and efficient way, e.g. the one that is close to him and not at maximum capacity yet.

A CDN could be distributed even more if the nodes do not have to be owned by the CDN operator itself. If the CDN node is actually a virtual machine that can be easily transferred from one cloud to another, the node could be placed even closer to the potential users. For this scenario to work well, it is necessary to have many potential locations for the nodes. The intercloud would be able to provide this.

6 CONCLUSIONS

This paper discussed the current state of cloud computing and showed that it is comparable to the state of networks before the internet. Clouds need to be connected more to make it easier for users to switch between providers and at the same time make it easier for providers to supply ”infinite resources”. Two cases were presented that would benefit from the intercloud: early warning systems and dynamic content delivery networks.

At the moment the big cloud providers do not feel the need to standardize this intercloud and there is no authorative body that sets the standard. It is necessary for the IETF to take its current effort to create a cloud reference framework one step further and standardize the interfaces between the functions and layers as well.

REFERENCES

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*.

Farinacci, D., Fuller, V., Meyer, D., and Lewis, D. (2009). Locator/id separation protocol (lisp). http://tools.ietf.org/html/draft-farinacci-lisp-12.

Hoff, C., Johnston, S., Reese, G., and Sapiro, B. (2010). Automated audit, assertion, assessment, and assurance api (a6). http://tools.ietf.org/id/draft-hoff-cloudaudit-00.html.

Karavettil, S., Khasnabish, B., So, N., Golovinsky, G., and Yu, M. (2010). Cloud security framework. http://trac.tools.ietf.org/area/app/trac/attachment/wiki/Clouds/Karavettil-et-al-CSF-Proposal-10Dec2010.pdf.

Khasnabish, B., Chu, J., Ma, S., Meng, Y., So, N., and Unbehagen, P. (2010). Cloud reference framework. http://www.ietf.org/id/draft-khasnabish-cloud-reference-framework-00.txt.

Mell, P. and Grance, T. (2009). The nist definition of cloud computing. http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

Parkhill, D. (1966). *The Challenge of the Computer Utility*. Addison-Wesley Publishing Company.