2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing

A Model for Accomplishing and Managing Dynamic Cloud Federations

Giuseppe Andronico*, Marco Fargetta*, Salvatore Monforte*, Maurizio Paone* and Massimo Villari†
*Istituto Nazionale di Fisica Nucleare, Sezione di Catania
Catania, Italy
Email: {giuseppe.andronico, marco.fargetta, salvatore.monforte, maurizio.paone}@ct.infn.it
†Università degli Studi di Messina
Messina, Italy
Email: mvillari@unime.it

***Abstract*—Cloud computing is not just a promising approach to the service provisioning: nowadays it represents the reference model in such field. Several cloud service providers have emerged as de facto standards and an increasing number of companies are choosing to migrate their business in the Cloud "ecosystem". Nevertheless, each provider adopts a particular interface to manage its services and uses a proprietary technology. In this paper we present a cloud federation model which is able to provide scalability and flexibility to small clouds. The idea is to benefit of renting seamless resources according to federation agreements among operators. The challenge here is to overcome all the problems raising trying to merge small clouds with heterogeneous administrative domains.**

***Keywords*—Cloud Computing, Cloud Federation, Dynamic Cloud Federations, Heterogeneous Systems**

I. Introduction

Nowadays, excluding the activities of several big cloud operators, small and medium clouds to increase the adoption of their services have to find solutions in the following cross cutting aspects: *auditability, availability, governance, interoperability, maintenance and versioning, performance, portability, privacy, regulatory, resiliency, reversibility, security, service levels and service level agreements*. These are strictly related with the well-known cloud deployment models such as *Public*, *Private*, *Hybrid* and *Community*, where the actors are *Cloud Service Customer (includes cloud service user)*, *Cloud Service Provider*, *Cloud Service Partner (includes cloud auditor and cloud service broker)* (see section III for further details). These aspects become more difficult to manage in wider scenarios where different operators trying to collaborate in models like Intercloud Interoperability and Federation. The *IEEE Standard Association* is working on Intercloud Interoperability and Federation with its project named *"P2302 - Standard for Intercloud Interoperability and Federation (SIIF)"* [1], which aims at developing standard methodologies for cloud-to-cloud interworking. It is interesting to see how the standard is defining the federation of clouds with common Addressing, Naming, Identity, Trust, Presence, Messaging, Time Domain, and Resource Semantics.

Practical approaches to federation does not supply with any clearly defined real example leading to some sort of semantic clash on what federation means. In other words, some clouds declare to be federated because of a shared file-system or other distributed or replicated service. This is not true and in order to understand the idea behind our approach it is important to keep in mind the following assertion: federation and resource sharing are two distinct concept with different meaning. So what is federation and what we want federated clouds act as? Let's start simply from a federation definition taken from a common dictionary:

> *Act of joining states or other groups with an agreement in common affairs they will be governed under one central authority.*

Translating this sentence into the cloud world is the idea underlain the proposed approach to federation, nothing is shared among federated clouds members, they have their own resources, users and autonomy but given the federation agreement they belongs to, each member supply the federation with its own resources.

In this work we describe a model of cloud federation able to provide scalability and flexibility to a group of small clouds. Although create a federation among small cloud operators with heterogeneous and different administration domains and technologies raises many problems, it should provide business benefits exceeding the drawbacks because they can compare with big cloud player, thanks to the possibility to rent seamless resources according to federation agreements among the federated operators. The work is in a preliminary stage, but it represents a starting point for investigating and formalising a model able to consider all implications in accomplishing and managing Dynamic Cloud Federations. The model, aimed at small cloud operators, allows them to easily join and leave the federation minimising all possible issues due to the evolving configurations. Moreover, the added-value of this work is in providing a concrete model that looks at heterogeneous cloud systems, in order to include in the federation different cloud middleware (e.g. OpenNebula, CloudStack, etc.).

The paper is organised as follows: Section II describes a brief survey on cloud federation models useful positioning our work respect to the State of the Art. Section III describes all terms and acronyms used in the paper. In Section IV, we make clearness on the concept of federation, distinguishing it from interoperability and orchestration, presenting the general idea of federation we are dealing with in this paper. Finally, our

Project CHAIN-REDS – European Community 7th FP Grant Agreement n. 306819, and Project PRISMA – IT PON program cod. PON04a2_A

978-1-4799-7881-6/14 $31.00 © 2014 IEEE
DOI

model is presented in Section V. Section VI concludes the work providing highlights for the future.

II. A survey on Cloud Federation Models

Cloud federation refers to mesh of clouds that are interconnected by using agreements and protocols necessary to provide a universal decentralized computing environment. Federation is raising many challenges in different research fields on cloud computing as discussed in [2][3][4] and [5]. Most of the works in the field concerns the study of architectural models able to efficiently support the collaboration between different cloud providers focusing on various aspects of the federation.

The FP7 European founded project RESERVOIR [6], which operates at IaaS introducing an abstraction layer allowing to develop a set of high level management components that are not tied to any specific environment. Therefore, several sites can share physical infrastructure resources creating a kind of federation, with the condition that all the involved clouds have a homogeneous environment. The experience acquired in RESERVOIR leads up to the latest EU initiative known as FI-Ware [7]. In particular, the EC is encouraging a federated framework based on Fi-Ware platform called XI-FI Federation [8]. Indeed, XI-FI federates homogeneous FI-Ware systems based on OpenStack framework. Here, it is interesting the work has been done in the area of formalization of federation cloud specifications, that is: *Federate Security*, *Federate Resources*, *Monitoring Resources* and *Define Scalability Rule*. However, XI-FI Federation maintains a static approach for making up the early phases of federation. XI-FI needs to formalize a-priory agreements among the cloud parties interested in joining the federation.

In the work of [9] the authors describe an architectural solution for federation by means of the Cross-Cloud Federation Manager (CCFM), a software component in charge of executing three main functionalities: i) discovery, which allows to exchange information on federated Clouds, ii) matchmaking, which performs the best choice of the provider that can loan its resources, and iii) authentication, to create a secure communication channel among federated Clouds.

Despite the obvious advantages, the implementation of a federated environment is not trivial at all. Even the OpenStack framework [10] is looking at the possibility to federate two or more OpenStack clouds. In particular, OpenStack initiative, is investigating on *Inter Cloud Resource Federation Models* as described into [11], where the InterCloud Resource Federation Alliance is formalized. In brief, the idea presented is to give partners investing in a joint venture the opportunities to make a bigger cloud entity with massive resources capacity. OpenStack foundation realized that security is one of the main challenge in cloud federation, as from the first item within the list of issues to be overcome in the presented assessments:

> *Security: as Tokens management, Single Sign On features, Resource Access Across Clouds, Data Export Control, etc.*

Therefore, researchers are looking at the possibility to federate users and policies as presented in Cloud Infrastructures [12] exploiting Virtual Organization Membership Service (VOMS) originally conceived for GRID computing. It is also interesting to see works trying to federate Keystones, the Identity and Access Management systems of OpenStack like reported in [13] and [14]. The complexity of Inter-cloud Architectures is well described in [15] where an architectural framework for cloud based infrastructure services provisioned on-demand is presented.

III. Terminology: Cloud Roles

Henceforth in text terms like *Cloud Service Providers (CSPs)*, *Service Providers (SPs)*, *Cloud Brokers (CBs)* and *Cloud Consumers (CCs)* will be used according with the NIST definitions [16]. Here we are considering CSPs at IaaS level, they can be persons, organizations, or entities responsible for making a service available to *Cloud Consumers (CCs)* in general. CSPs provision the physical processing, storage, networking, and other fundamental computing resources. Hence, SPs deploy, configure, maintain, and update the operation of the software applications on a cloud infrastructure at PaaS and SaaS levels. Indeed, at IaaS level, CCs exploiting CSPs can accomplish services for both PaaS and SaaS layers. Here we are considering these CCs relying as SPs. Customers use application/service for business process operations interacting only with SaaS services through SPs. The relation among these actors is:

$$CSPs \Longrightarrow SPs \Longrightarrow Customers$$

NIST defines a *Cloud Broker* as an entity that manages the use, performance, and delivery of cloud services, as well as negotiates relationships between CSPs and SPs.

A home cloud, in order to lease resources on foreign clouds, has to assume a role of tenant for foreign clouds. Here, a *Tenant* is defined as the temporary virtual resources owner. In particular in our context with the term *Tenant* we refer to a set of resources with related access policies and users.

The cloud federation scenarios have also introduced new terms for simplifying the overall description when more stakeholders are considered. Whenever a small cloud wants to increase its capabilities can initiate all federation procedures against an external cloud operator, relying as a target for the requests. SNIA for dealing with Federation and Cloud Storage (see CDMI [17]) introduced the concept of *Federation Initiator* and *Federation Target*. In a context of complex and explicit federation boards/platforms/alliances where agreements are formalized for guarantying policies and rules it is better to refer to *home clouds* and *foreign clouds*. Whenever a home cloud needs to expand its capabilities asks to the federation alliance in which one of the partner cloud fulfills the request; it relies on a foreign cloud. In OpenStack federation model a Federation Alliance is defined as reported in [11]. Our work follows this latter similar approach having an explicit federation board/alliance. In cloud federation others terms are coined as well as: *Federator and/or Federation Agent* and *CloudFederationAuditor* (`CFA`). The former is a module/component inside each cloud, in charge for actuating the federation procedures inside the alliance communicating with all other home and foreign cloud agents. The latter is a third-part entity in charge for actuating the overall federation procedures inside the alliance communicating with all the Federators.

IV. Reference Scenario

To face the issues concerning *cloud federation*, two aspects have been isolated and investigated separately by the scientific community. One aspect focuses on cloud interoperability, which mostly consist in the action of devising protocols able to access cloud services on different software systems (e.g., OpenStack, OpenNebula, EC2, etc.), thus the main effort is devoted to the design communication protocols and resources dissemination policies (e.g the EGI federated cloud [18]). This activity has involved several standardisation organisation and produced standards like OCCI [19] and others. The other aspect deals with the definition of the entities operating in the *Cloud Federation* (linked to the roles described in section III), and the actions these entities need to perform in order to manage the system (e.g.: Federation joining, service negotiation, SLA monitoring, etc.).

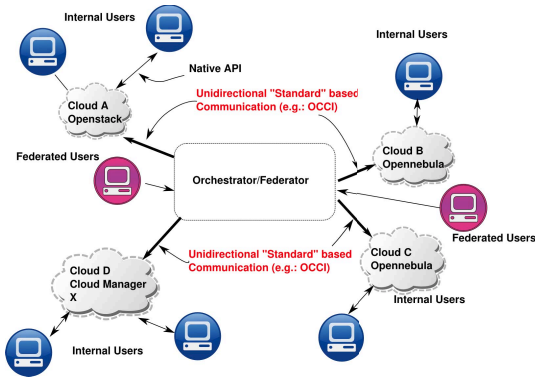

Fig. 1. Centralized approach to the federation: the users requests are translated and forwarded to external CSPs by a central entity.

In our opinion, the approach focused on interoperability requires a centralised entity which receives requests from a CC that have to access the federated cloud resources and translates them into requests to external CSPs (see Figure 1). Actually, this model is not a cloud federation following the definition presented in this paper, since users are aware of the different CSPs and there is not cooperation among CSPs. Generally, this approach will imply that users need to adopt different software interfaces to access either their own internal resources or the external ones offered by "federated" sites. Hence, users are divided in *internal users* and *federated users*: the former access cloud services through native APIs, whereas the latter interact with the central entity through federation specific APIs. This simplification of federation presents some issues that can be critical in specific scenarios. Internal users cannot extend their cloud resources by taking advantage of federated CSPs, because they need another external software system that, in turn, will access resources not related to their own cloud. Additionally, internal users may have applications developed on cloud manager specific APIs thus in order to exploit the federated resources such applications have to be rebuilt. Nevertheless, each cloud may provide different services or interfaces (e.g. event notification or monitoring service), which cannot be available on the federation system.

Differently, the approach focused on the entities definition, as described above, allows to design a system able to transparently extend each cloud including external resources. Figure 2 depicts a simple scheme of such a system. This model implies no distinction between internal and federated users: it defines only *cloud users*, which can access the resources offered by both their own CSP and external federated ones through cloud native interfaces. Most of the harmonization work among the federated CSPs is performed by software running on each site (represented by the FedGW graphical block in the Figure). The entity Federator will carry out operations like resource discovery, marketplace of image templates, and so on.

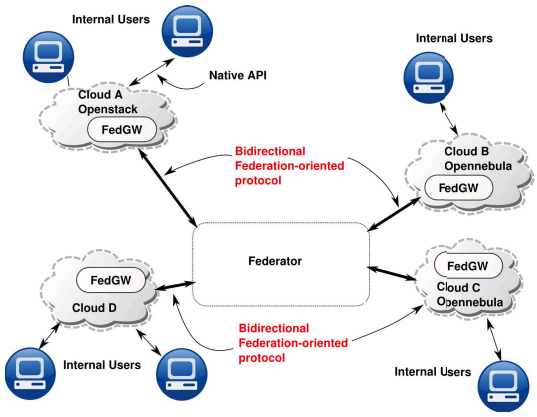

Fig. 2. An user-transparent approach to federation: each cloud extends its resource using external federated resources

To better understand the roles played by each actor let us consider the scenario depicted in Figure 3, where clouds A, B and C are small CPSs, whereas clouds D and E are big enough to internally address any request. CSP D is distributed around the world and its internal interconnection is depicted (link between D and D').

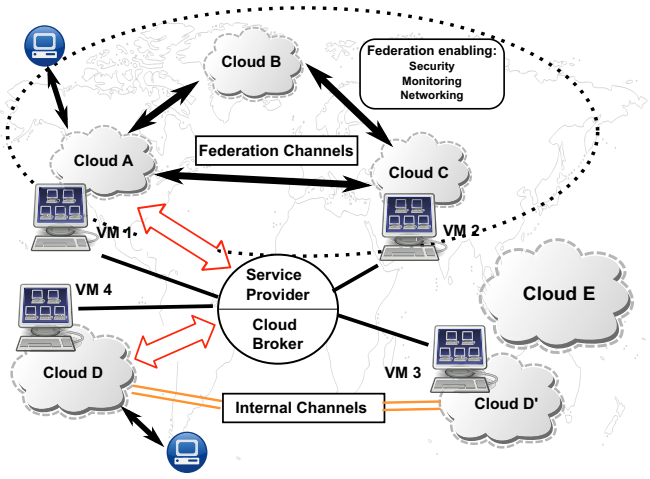

Fig. 3. IaaS: Scenario with stand-alone Clouds(D and E), Federated Clouds (A, B and C) and Cloud Brokers, Service Providers, and Customers. Highlights of *In-Federation and Internal Channels*. Moreover Cloud Customers interacting respectively with Cloud A and Cloud D.

Cloud brokers act as third part intermediary agents, that make their business selecting the best solution satisfying both

the CSPs and SPs' requirements. Our interest is to provide clouds A, B and C the same type of business opportunities as for clouds D and E, in which neither brokers nor SPs might be aware of the capabilities each cloud operator supply with.

In this work we analyse the steps required to define a federation agreement under which the cloud operators A, B and C can cooperate maintaining different administration domains. The model presented next treats all the solutions in a general way, hence they can be used also for different cloud middleware (e.g. OpenStack, OpenNebula, CloudStack, etc.).

CSPs have the flexibility to join more federations without restriction and in a flexible way, that is, some CSPs can setup one or more types of federation with different goals such as green policies, low cost offerings, high availability and so on.

Since the federation does not involve neither SPs nor CBs it is necessary to setup a common federation framework where all rules and policies are respected. This transparency makes the task difficult considering issues such as compound SLAs (i.e. final SLAs towards SPs is made from a composition of more SLAs) or different network facilities. However, despite the complexity such a federated environment allows CSPs to make new business leveraging their internal infrastructure, but also external renting resource. Thus, each CSP is able to satisfy their customers demands and making profit of unemployed resources by providing them to other CSPs.

One cloud with many datacentres can be represented as one domain entity with many communication channels, here named *Internal-base*, governed by same network policies and rules. The federation needs to setup the equivalent communication channels, here named *In-Federation-base*, governed by different network policies and rules. The challenge is exposing the same behaviour to cloud brokers and service providers actors even if cloud operators are totally different. Figure 3 also shows these two possible configurations, where the encircled clouds A, B and C constitute the cloud federation. Cloud brokers and service providers can interact with either cloud A or D, accessing respectively a federation of clouds or a distributed datacentre. Looking at the picture a SP can indifferently exploit resources in the configuration reported in top part of the picture as well as in the bottom part. The bottom part is equivalent to a generic public cloud service like Amazon operator. The picture shows that VM3 and VM4 represent two instances running for example in US and in Australia communicating on a proprietary channel established by the operator. In the top part of the picture another SP can have the same type of VMs but executed in small cloud operators. In particular, the picture shows VM1 and VM2 running for example in Canada and in Japan respectively where the communication channel is established by the two members under the federation agreement defining policies and QoS.

We remark the compelling work here is to investigate and formalise a model able to consider all implications required to accomplish the latter solution. Section V provides all highlights for overcome the problems just discussed above, trying to minimise all issues due to the evolving configurations of networks, security and monitoring parts and so on.

V. Proposed Cloud Federation Model

In section IV several approaches to cloud federation have been presented, each and every one having different peculiarities. Nevertheless, none of them comply with our interpretation of the federation leading us to define our own reference model.

According with our model cloud federation life cycle comprises of two distinct moments: join/exit and the resources access. The former is related to the activities performed by a CSP to create or destroy the environment needed by the federation members to communicate each others. The latter is related to the discovery, negotiation and usage of federated resources. The relation between the two moments as well as the actors involved is shown in figure 4.

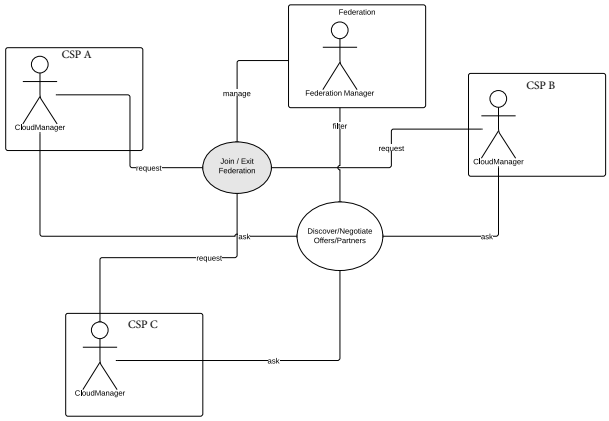

Fig. 4. Cloud Federation model - Use Case

To join a federation the CSP has to follow several steps as shown in the state diagram depicted in figure 5. In the first state the joining CSP contacts the federation manager sending information about the resources (e.g. cores, storage, etc.) which might potentially be available to the federation parties as well as usage policies on those resources. Federated resources are not dedicated for exclusive use by the federation members but these are upper bounds of the resources available and its real usage depends on the actual request during federation life cycle.

The federation manager, upon join request reception, checks whether the information provided about resources and policies matches with the federation rules or not. If the request is accepted the just joining member is instructed to create a *tenant* with the resources declared in the join request. At this point the CSP can be considered as being federated and ready to fulfil requests from/to others federation members.

A CSP can modify the amount of resources committed to the federation and the policy in any moment but the changes must be notified in advance to the federation manager, who will propagate the information to all members. Obviously, during the information update the federation can reject a member because it does not comply any more with the rules. A CSP can leave the federation, either for its or the federation manager decision. The federated CSP cannot leave immediately since some resources might be committed and still used, therefore the CSP enters in a leaving state. This state will terminate when

all the resources are free or if the leaving period defined in the join agreement has expired, in this case the resource will be forcibly released and remaining data or services discarded. The federation manger notifies all the members about the current disconnection of the CSP. The members have to release the resources the leaving CSP supply with before expiring of a given timeout period.

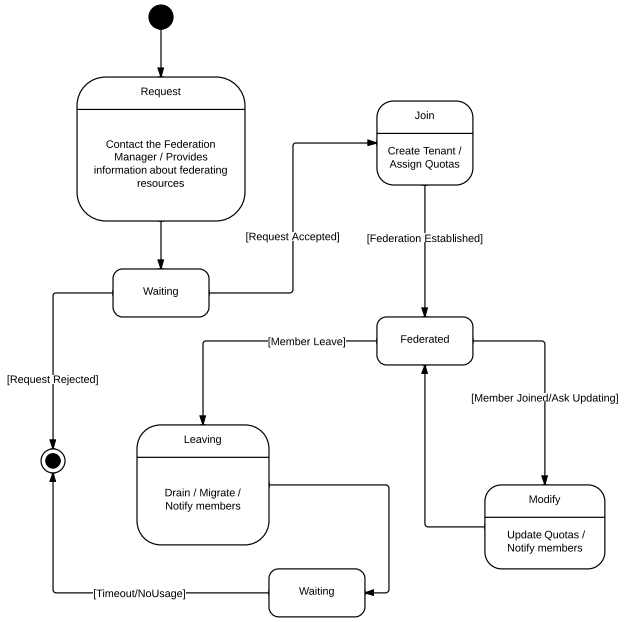

Fig. 5. Join and exit federation - State Diagram

The federation defines the technical aspects in order to access remote resources and maintains a list of CSPs providing resources with both qualitative and quantitative information. Nevertheless, in order to access member resources a new negotiation is requested between the two members, acting one as CSC and the other as CSP, with the supervision of the federation manager acting as CFA. Figure 6 shows the state diagram related with the discovery and negotiation of federated resources.

To access federated resources the cloud manager has to send a request to the federation manager including the list of requested resources (e.g. number of cores, storage or other) and specify an optimisation function used to pick the best fit among the possible results the CSPs supply with[1]. The optimisation function contains constraints related to the resources, like performance, location, reliability, etc. . . as well as parameters describing QoS / SLA constrains. The federation manager, upon reception of the request, queries the members able to provide the relevant resources based on the information published in the federation about current availability and prices. The optimisation function is then applied to select the best fit for the waiting CSC. This activity is performed automatically and unattended so it does not require any human interaction.

The cloud manager can reject the offer selected by the

[1]The request is an XML document based on WSAgreement and include RDF elements for resource description.

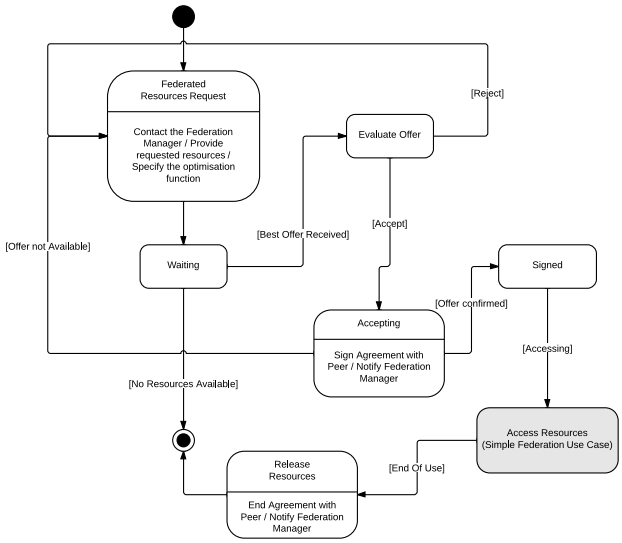

Fig. 6. Discovery and negotiate federated resources - State Diagram

federation manager and then could send a new request with a different optimisation function. If the offer is accepted an agreement has to be established before the CSC can access the resources. The agreement is an XML document based on WSAgreement [20], which has to be signed by the two parties and the federation because it is responsible for all the relations among its members. Therefore, the federation manager is notified when the agreement takes place and is over, as well. This allows the federation manger to have full knowledge of the resources usage among the members and implements strategies for a better distribution and optimisation of workload in the federation.

After the agreement is signed the CSC can start deploying services on the resources of the CSP, upon user requests. The deploy and access to remote resources by the user is shown in Figure 7 and described below. Resources under the agreement are reserved to the CSC and cannot be used by the owner.

During normal operation, shown in Figure 7, when a cloud user, or any CSC, requires new resources the cloud manager discriminate whether these will be provided as internal resources or taken from the federation. In the former scenario resources are managed by the CSP as usual. In case of federated resources the cloud manager will become a CSC of the federation and will start the negotiation procedure described above. These operation are internally managed by a federation agent inside the cloud. Upon agreement establishment, the required resources are committed in the remote CSP and the relevant endpoints sent to the federation agent who will activate a mapping service to generate local endpoints for the users. The mapping is requested to masquerade the real location of the services. As a result, the user can access the services transparently as resources managed by the cloud itself, hiding to the user the real owner of the resources and their location, which is an important aspect of the federation.

Finally, agreements could be defined in advance, before users request new resources. Moreover, users might release

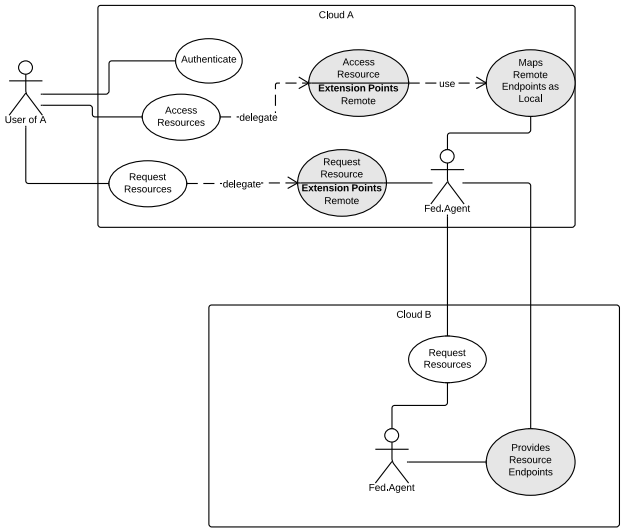

Fig. 7. Request and access federated resources - Use Case

requested resources before the actual expiration of the corresponding agreement, thus leaving them unused within the owning cloud. Hence, internal policies of federated resources usage should be defined and pursued by each member.

VI. Conclusion and Future Work

In this paper we have presented the idea of cloud cooperation among operators based on federation agreements. The challenge we want to address with the federation is to overcome all the problems raising in merging clouds with heterogeneous administration domains. Therefore, we introduced a high level model of cloud federation able to provide the scalability and flexibility needed by small clouds. The added-value of this work is in providing a high-level model not related to a specific technology which aims at federating different cloud infrastructures.

For the future we are looking at a concrete implementation useful for testing the goodness of our model, but also for providing new features and solving real problems that may occur in cloud federation accomplishments.

References

[1] IEEE, "P2302 - the ieee standards association," http://standards.ieee.org/develop/project/2302.html, 2014.

[2] F. Tusa, A. Celesti, M. Villari, and A. Puliafito, "How to enhance cloud architectures to enable cross-federation," in *Proceedings of IEEE CLOUD '10*. IEEE, July 2010, pp. 337–345.

[3] G. Vernik, A. Shulman-Peleg, S. Dippl, C. Formisano, M. Jaeger, E. Kolodner, and M. Villari, "Data on-boarding in federated storage clouds," in *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*, June 2013, pp. 244–251.

[4] I. Goiri, J. Guitart, and J. Torres, "Characterizing cloud federation for enhancing providers' profit," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, july 2010, pp. 123 –130.

[5] S. Azodolmolky, P. Wieder, and R. Yahyapour, "Cloud computing networking: challenges and opportunities for innovations," *Communications Magazine, IEEE*, vol. 51, no. 7, pp. 54–62, July 2013.

[6] B. Rochwerger, D. Breitgand, A. Epstein, D. Hadas, I. Loy, K. Nagin, J. Tordsson, C. Ragusa, M. Villari, S. Clayman, E. Levy, A. Maraschini, P. Massonet, H. Munoz, and G. Toffetti, "Reservoir - when one cloud is not enough," *Computer*, vol. 44, pp. 44–51, 2011.

[7] FI-WARE, "Open APIs for Open Minds," http://www.fi-ware.org, 2014.

[8] FI-XIFI, "Joining The Federation Scenario Exploiting FI-Ware framework," http://wiki.fi-xifi.eu/Public:Joining_the_Federation_scenario, 2014.

[9] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Three-phase cross-cloud federation model: The cloud sso authentication," in *Proceedings of the 2010 Second International Conference on Advances in Future Internet*, ser. AFIN '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 94–101.

[10] "The open source, open standards cloud, innovative, open source cloud computing software for building reliable cloud infrastructure. http://openstack.org/ jan 2014." [Online]. Available: http://openstack.org/

[11] OpenStack Inter Cloud Resource Federation. https://wiki.openstack.org/wiki/InterCloudResourceFederation, 2014.

[12] A. Lopez Garcia, E. Fernandez-del Castillo, and M. Puel, "Identity federation with voms in cloud infrastructures," in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, vol. 1, Dec 2013, pp. 42–48.

[13] D. Sitaram, H. Phalachandra, A. Vishwanath, P. Ramesh, M. Prashanth, A. G. Joshi, A. R. Desai, H. P. C. R, Prafulla, S. R, and Y. A, "Keystone federated security," in *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*, Dec 2013, pp. 659–664.

[14] D. Chadwick, K. Siu, C. Lee, Y. Fouillat, and D. Germonville, "Adding federated identity management to openstack," *Journal of Grid Computing*, vol. 12, no. 1, pp. 3–27, 2014. [Online]. Available: http://dx.doi.org/10.1007/s10723-013-9283-2

[15] Y. Demchenko, C. Ngo, C. de Laat, M. X. Makkes, and R. J. Strijkers, "Intercloud architecture framework for heterogeneous multi-provider cloud based infrastructure services provisioning," *IJNGC*, vol. 4, no. 2, 2013.

[16] NIST, "Nist cloud computing standards radmap," http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf, 2013.

[17] SNIA, "Cdmi and cloud federation," http://www.snia.org/sites/default/files2/SDC2012/presentations/Cloud/DavidSlik_Federations_Year_3_R2.pdf, 2012.

[18] European Grid Infrastructure, "Egi federated cloud," https://www.egi.eu/infrastructure/cloud/.

[19] Open Grid Forum, "An Open Community Leading Cloud," http://occi-wg.org/.

[20] ——, "Web Services Agreement Specification (WS-Agreement)," https://www.ogf.org/ogf/doku.php/documents/documents, 2007 (update 2011), GFD-R.192 (Obsoletes GFD.107).