Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 15 Issue 2 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Issues in a Scalable Inter Cloud Environment with Unified Brokering Approach

By Bhawna Taneja & Dr. Rajender Nath
Kurukshetra University, India

Abstract- Cloud Computing providers are currently serving customers throughout the world. Inter-Cloud Computing, where a number of providers come together, has already paved its way, It is meant to address the growing challenges of load balancing and optimal utilization of resources. At the same time, its objectives also include QoS and SLA accomplishment.

A centralized Federation of clouds is a confederacy of cloud providers attached to and dependent upon a single unified broker entity. This unified broker acts as a linchpin for the entire system.

This paper envisions and elaborates upon the idea of centralized Inter-cloud federation environment. We propose issues open to centralized Inter-Clouds at two levels namely unified broker and the cloud providers.

Keywords: *qos, sla, inter-cloud computing, broker, centralized federation of clouds.*

GJCST-B Classification : *C.1.4, C.2.1*

Strictly as per the compliance and regulations of:

Issues in a Scalable Inter Cloud Environment with Unified Brokering Approach

Bhawna Taneja [α] & Dr. Rajender Nath [σ]

Abstract- Cloud Computing providers are currently serving customers throughout the world. Inter-Cloud Computing, where a number of providers come together, has already paved its way, It is meant to address the growing challenges of load balancing and optimal utilization of resources. At the same time, its objectives also include QoS and SLA accomplishment.

A centralized Federation of clouds is a confederacy of cloud providers attached to and dependent upon a single unified broker entity. This unified broker acts as a linchpin for the entire system.

This paper envisions and elaborates upon the idea of centralized Inter-cloud federation environment. We propose issues open to centralized Inter-Clouds at two levels namely unified broker and the cloud providers.

Keywords: QoS, SLA, inter-cloud computing, broker, centralized federation of clouds.

I. Introduction

Cloud Computing is a relatively new paradigm in the history of computing. Cloud computing offers services and computing resources over the most common medium of access and communication i.e. Internet in a pay-per-use basis. Numerous authors have defined the term "Cloud Computing" in their own ways. The most acceptable and standardized definition out of these turns out to be that by National Institute of Standards and Technology (NIST) [8]: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Most common characteristics of Cloud Computing paradigm are on-demand access to resources, scalability, ubiquitous network access, multi-tenancy, metered service, elasticity etc. Cloud Computing has a layered architecture with IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) as its layers.

Next leap in the history of Cloud Computing has already made its way and it involves association between various Cloud Providers to efficiently and impeccably render their services to the Cloud Consumers. When a Cloud Provider serves a number of consumers, sometimes load becomes more than it can be provisioned. Under such circumstances, some of the consumers are denied of services and the overall response time increases. This leads to loss of trust and poor SLA accomplishment. Less optimum but still a solution is, to increase the infrastructure. But this infrastructure remains idle most of the time when the workload is at its average rate. To optimally utilize the infrastructure and to reduce the response time, Inter-Clouds have come up, where one Cloud provider can utilize the resources of other Cloud Providers. This is especially useful in case of heavy load and also during Cloud outages. Inter-Cloud is a generic term used for all types of associations between various Cloud Providers. This association can take various forms. The federation of clouds can either be peer-to-peer federation of clouds or centralized federation of clouds [1]. In a peer-to-peer federation, each cloud provider has its own broker resulting in a distributed association of cloud providers. In a centralized federation (fig. 1), there is a single broker entity and all the cloud providers publish their SLAs to this unified broker. This broker entity acts as a mediator between cloud consumer and multiple interoperable cloud providers. Broker matches the specifications (QoS, cost etc.) of the consumer request with providers' SLAs and allocates the best fit to the consumer.

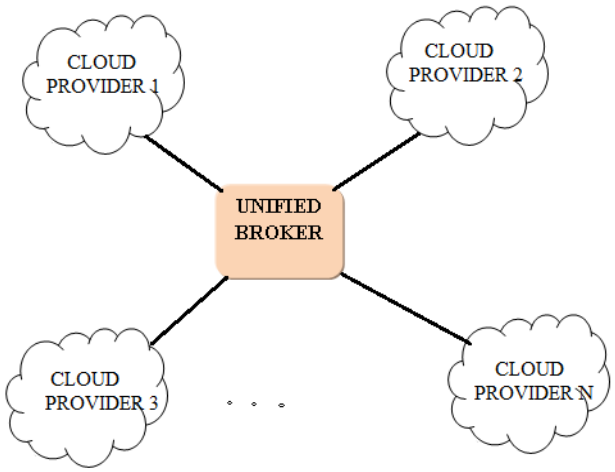

Figure 1 : Centralized Federation of Clouds

Author α : Bhawna Taneja, Research scholar, DCSA, Kurukshetra university, Kurukshetra e-mail: tanejabhawna@gmail.com
Author σ : Rajender Nath, Professor, DCSA, Kurukshetra University, Kurukshetra. e-mail: rnath2k3@gmail.com

In this paper, focus is primarily on centralized federation of clouds and various issues associated to the adoption of such an environment have been investigated.

II. Related Work

The assessment of the requirements for successful implementation of federation of clouds has been undertaken by many authors in the recent past. This section investigates the challenges identified by researchers in centralized federation of clouds.

Authors [2] in their paper addressed the issues in implementing the multiple data management system on a cloud such as hardware asymmetry, reliability and dynamic resource sharing as per application's requirement.

In paper [11] proposed incorporating concepts of Grid technologies to realize multi cloud federated deployments. According to them, solutions from Grid technologies in terms of compute, data, security and information system areas can not be directly applied to federated cloud computing and hence require some integration efforts to find a solution to these problems.

The challenge of identity management in federated cloud environment has been emphasized by [3]. They also compare the security models in Grid and CC. Authors also described inter-cloud federation scenarios and identity management in it.

The security risks in a cloud federation and the need to deal with these threats have been highlighted in [16]. In federated cloud environment, this responsibility of maintaining the security is split amongst various CPs. Auditing multiple CPs ma become a trivial task when customer may not even be aware of existence of multiple CPs. There are liabilities and legal issues too involved in federated cloud environment especially in case of failure or downtime.

The authors in the paper [12] have pointed out the deployment models for linking together Network Enterprises together i.e. while forming the federation of clouds. They also listed the probable challenges related to interoperability issue.

The benefits of moving from proprietary cloud-based applications to inter-cloud computing have been enumerated by authors [9]. Due to legislative reasons or response time constraints, a consumer may want to store data at a nearest or a particular data center. It is not possible for a cloud provider to have data centers at every location across the globe. The solution to this problem is using multiple clouds. Secondly, inter-cloud computing also results in better application resilience due to more service availability even in case of cloud outages. Another benefit cited by them is vendor lock-in", is avoided since same workload can be shared among multiple cloud providers. Cloud vendors are equally benefited by being able to scale-up their resources whenever workload is bursty and increases beyond their limits.

III. Issues under Apprehension in Centralized Cloud Federation

The success of any federation of cloud providers depends on its management and control over its components at different layers of cloud architecture. There are two entities in the centralized federated system namely cloud broker and the cloud providers to do this. To raise the confidence of customers in centralized cloud federation, the broker and a cloud provider need to overcome all technical issues that are critical to resource prediction, resource allocation, transparent accounting, location and identity etc.

a) Issues from broker perspective

The centralized cloud federation depends on unified resource broker for resource allocation since at the heart of centralized federation lies the broker. The broker intercepts the requests from cloud consumers along with their service level requirements (e.g. response time, Bandwidth requirements, cost etc.). Efficient scheduling algorithms need to be enforced to match the consumer requests with the SLAs published by various cloud providers [6]. As many applications run in parallel, broker has to maintain the complex accounting of each provider and customer in a federated cloud environment. Some of them are transferred from one cloud provider to another amidst their execution (VM images and associated data structures are transferred from one cloud provider to another). Competent data structures and procedures for accounting of these applications (partly or completely executed) are also necessary to be developed at the broker level.

In a centralized federated environment, broker introduces the cloud consumer to its suitable cloud provider after SLAs match. Maintaining the transparency to the user about his effective provider lies on the shoulders of broker and it has to maintain the continuous transparency even if there is a shift in cloud provider before the job completion/execution [5]. The location of data is visible to cloud provider and not to the consumer. This problem of location awareness increases multi fold in federated cloud environment since data is transferred to multiple cloud providers during service compliance. As data is most vital asset to the owner data location awareness procedures for this purpose must be developed at the broker level [7].

VM Migration scenario too requires due diligence that occurs quite frequently in federated environment due to depletion of resources at one cloud provider or due to a cloud outage (of a member cloud). Partially executed services may have to be transferred from one provider to another. Virtual machine images need to be handed over to recipient cloud provider so

that cloud consumer doesn't encounter undue delays. The arrival pattern of the requests for cloud services can serve as an important metric, if analyzed properly. In order to avoid under-provisioning of resources, the broker has to develop some behavior prediction metrics to predict the no. of required resources for each request. These metrics may be developed after a careful study of the consumer requests for a certain period of time [1]. Another very important area from a broker's perspective is Identity management. In order to effectively utilize the power of federated cloud environment, the efficient management of identities has to be established. The federated identity provider should employ a single, common but secure identity to access the applications between different providers. The federated identity manager should have flexible but extensible architecture to enforce identity security policies and yet be light weight [14].

b) Issues from cloud provider perspective

Undoubtedly, the hesitation in adoption of federated cloud environment can only be fully alleviated or minimized if each participating member cloud provider properly attends the issues pertaining to its efficient service delivery, integrity of data, etc.

A member cloud provider in centralized federation of clouds needs uniform and automated authorization mechanisms. A cloud provider has to authorize the cloud consumer before any actual usage of the cloud service begins. In a federation, such authorization mechanisms need to be enforced which are identical with every cloud provider. Automated authentication methods must be contained which rarely obstruct the execution of the service being rendered to the consumer [10]. A single cloud provider serves many cloud consumers. It is the foremost responsibility of cloud provider to ensure integrity and confidentiality of data of each cloud consumer whether at disk or "on wire". Consumer must be made aware of the data location and assured about its integrity [4].

Each cloud provider always wishes to avail the maximum of profit by delivering the full services to its customer. But this may not happen in case the available resources are under-provisioned and this may entail the decomposition of the request into smaller requests by the provider. Hence, only some of these required small portions of requests may be outsourced by the provider and fulfilling the larger request itself. This process of disintegration of request and transferring the workload to other cloud for completion requires vigilant and rational algorithms which actually enhance the throughput and reduce the response time [13]. While service decomposition process, a cloud provider has to ensure implementing concurrency control since it handles many service requests from different cloud consumers simultaneously. This may use same storage area for local storage of data. Thus it becomes indispensable on the part of cloud provider to provide locking measures to ensure concurrency control. A cloud provider needs to have sound recovery mechanisms. If any of the member cloud provider faces outage, the decisive question that arises is what will happen to the vital data of cloud consumers. A need evolves to replicate the data. A decision needs to be taken by the cloud provider regarding the degree of replication i.e. whether the Cloud provider should opt for full replication or not. Second problem is that of dealing with consumer requests in case of cloud outage. Cloud Broker can reschedule the services provided by such cloud providers till they are up and functional again. The performance of federation is also questionable in case unified broker goes down for any unforeseen reason [15].

Since the federation is made up of independently managed clouds and infrastructure of different administrative domains. So, the federated Inter-Cloud system must be able to specify such inter-cloud gateway translators which support conversion of requests, pattern or formats of data (at SaaS level) and underlying protocols (at IaaS level) from one to another cloud domain [4]. The federation has to confront and support inter-application synchronization and run time infrastructure optimization which includes migration of Virtual Machines from one provider to another, ability to handle new joining/leaving of VMs and resource scaling in harmony with the job's need.

IV. Conclusion and Future Work

This paper examined the idea of centralized federation of cloud providers with a view to provide a deeper look into the requirements of inter-cloud federation. The issues addressed above are of higher relative importance from the broker's point of view and from provider's angle. The outcomes of this research revelation, if properly attended, will give significant strength to the centralized federation of cloud providers. The different issues have been highlighted at various layers of the cloud (SaaS, PaaS and especially at IaaS level). It also allows the providers to assess the effort that is required to integrate the existing cloud computing systems with a federation of clouds. The federation can work in a collaborative manner only if unified broker carries all of its above mentioned responsibilities with due respect. The timely and regular publishing of SLAs, optimizing the load distribution and run time infrastructure optimization are critical factors for retaining the customer. In this work, only equi-probable events (like cloud outage, resource depletion etc.) are assumed to happen. If the relative weightage of each issue is also considered then scenario may become more complicated and a statistical analysis may also be greatly helpful.

The future objective of this research will be on developing the comprehensive solutions to come across these above mentioned issues. These findings will lead to figure out the robust architecture which may be integrated into the existing model. A deeper look into the inter-cloud security mechanisms, legal understanding, monitoring, fixing the responsibilities are other areas of further interest. Undoubtedly, the strength of the cloud providers is really elevated to new heights if they work in a federation of cloud like architecture but it is also evident that these peaks may be maintained only if the issues highlighted in this paper are addressed properly.

References Références Referencias

1. Buyya, R., Ranjan, R., & Calheiros, R. N. (2010). Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. In Algorithms and architectures for parallel processing (pp. 13-31). Springer Berlin Heidelberg.
2. Chen, G., Jagadish, H. V., Jiang, D., Maier, D., Ooi, B. C., Tan, K., & Tan, W. (2014). Federation in cloud data management: Challenges and opportunities. Knowledge and Data Engineering, IEEE Transactions on, 26(7), 1670-1678.
3. Demchenko, Y., Ngo, C., de Laat, C., & Lee, C. (2014, March). "Federated Access Control in Heterogeneous Intercloud Environment: Basic Models and Architecture Patterns", In Cloud Engineering (IC2E), 2014 IEEE International Conference on (pp. 439-445). IEEE.
4. Demchenko, Y., Makkes, M. X., Strijkers, R. J., & de Laat, C. (2012, December). Intercloud Architecture for interoperability and integration. InCloudCom (pp. 666-674).
5. DMTF (Distributed Management Task force) Inc., White Paper "Interoperable Clouds", 2009.
6. GICTF (Global Inter-Cloud Technology) Forum, "Use Cases and Functional Requirements for Inter-Cloud Computing", August 2010.
7. GICTF (Global Inter-Cloud Technology) Forum, White Paper "Technical Requirements for Supporting the Intercloud Networking", 2012.
8. Grance, T. (2010), "The NIST cloud definition framework", National Institute of Standards and Technology, Gaithersburg, MA, USA.
9. Grozev, N., & Buyya, R. (2014). Inter-Cloud architectures and application brokering: taxonomy and survey. Software: Practice and Experience, 44(3), 369-390.
10. Li, W., & Ping, L. (2009). Trust model to enhance security and interoperability of cloud environment. In Cloud Computing (pp. 69-79). Springer Berlin Heidelberg.
11. Memon, S., Rybicki, J., Riedel, M., & Yen, E. (2012, May), "Bridging the gaps: Federation of Clouds using Grid services and standards", In MIPRO, 2012 Proceedings of the 35th International Convention (pp. 411-416). IEEE.
12. Mezgár, I., & Rauschecker, U. (2014), "The challenge of networked enterprises for cloud computing interoperability". Computers in Industry, 65(4), 657-674.
13. Nodehi, T., Ghimire, S., Jardim-Goncalves, R., & Grilo, A. (2013). On MDA-SOA based Intercloud Interoperability framework. Computational Methods in Social Sciences (CMSS), 1(1), 5-22.
14. Núñez, D., Agudo, I., Drogkaris, P., & Gritzalis, S. (2011). Identity management challenges for intercloud applications. In Secure and Trust Computing, Data Management, and Applications (pp. 198-204). Springer Berlin Heidelberg.
15. Tsuda, H., Matsuo, A., Abiru, K., & Hasebe, T. (2012). Inter-cloud data security for secure cloud-based business collaborations. Fujitsu Sci Technol J, 48(2), 169-176.
16. Undheim, A., Meland, P. H., Bernsmed, K., & Jaatun, M. G. (2012, December). "Thunder in the Clouds: Security challenges and solutions for federated Clouds", In Proceedings of the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 113-120). IEEE Computer Society.