# Having Centralized Monitoring as a Service in Cloud Computing: A Study of Performance Aspects

Ajay Prasad
University of Petroleum and Energy Studies
Dehradun, India

Prasun Chakrabarti
Sir Padampat Singhania University
Udaipur, India

## ABSTRACT

A Centralized Monitoring as a Service (CMaaS) is a desired and necessary feature to be included in cloud computing. One of the concerns in having CMaaS from both user and provider's perspectives would be that of performance implications. Carrying out a performance analysis thus, becomes an important task before suggesting a MaaS solution. A straight forward performance study would be to find out whether the inclusion of monitoring processes affects the normal user request processing or not. The paper studies the affects by forming a simulation environment. The studies will also help datacenters in deciding whether to have dedicated VMs allocated for monitoring or to have monitoring processes share the VMs allocated for processing user requests.

## Keywords

cloud computing, monitoring, Access management, MaaS, Centralized MaaS, Performance study.

## 1. INTRODUCTION

We will at first discuss the need of a centralized monitoring in cloud environments followed by an overview model of centralized Monitoring as a Service(CMaaS). Next, we will be discussing the topologies and simulation environments. Finally, an analysis of the results and conclusive remarks will be presented.

### 1.1 Cloud issues: Monitoring and auditing

In cloud computing, access management, monitoring and auditing are highlighted as major concerns and issues by most of latest researchers [1-4]. In fact, Ali Khajeh Hosseni and colleagues [1] went further to mention that controlling and managing organizational employees as end users will also be an issue worth discussing. CSA [5] points out the need for logging control and access activities. Our observation is that the aspect of putting monitoring in the context of authorization will help in auditing in many ways. Spring J [6] stressed that long term monitoring can help extensive forensics as well as manageability. Thus, it is understood that the users must be given the choice of Monitoring as a Service (MaaS). Monitoring in access management will also add to the trust value [7] between users and the providers.

### 1.2 Basic requirements of a MaaS:

Basically, the monitoring as a service should have following properties in order to be efficient:

1. Substantial repositories.
2. Long term monitoring.
3. Verifiable monitoring.
4. Consistent time stamping.
5. Minimal cost overheads.
6. Minimal performance implications on the services.

Repositories have to be maintained to keep records for long durations as well as the repositories has to be maintained at both sides (users and providers). Consistent and appropriate time stamping [8] has to be provided whereby the digital signatures [9] can be formulated to verify logs holding time stamps. The system must provide mechanisms and functions to verify logs, so that, the logs can't be manipulated for vested interests and other reasons. This verifiability will also ensure high credibility and audit-ability to the either sides. However, including monitoring will certainly affect the overall performance implications to the users. So far no analysis has been made in the lines of performance implications of centralized, long term and verifiable monitoring in clouds. This needs to be done.

## 2. GENERIC MAAS MODEL

A generic CMaaS model can be viewed as a middleware at both user site as well as cloud provider site. As shown in figure 1a the monitoring is an independent module which processes the access requests to and fro from end users to the middleware authentication and authorization. The access management will be responsible to maintain roles and policies repositories along with monitoring reports and logs. The middleware at every user node will be responsible to authenticate and authorize [10] only after forwarded by monitors.

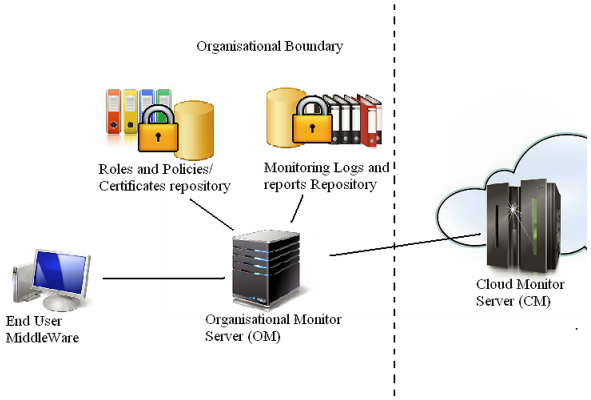


**Figure 1a: Monitoring at organization**

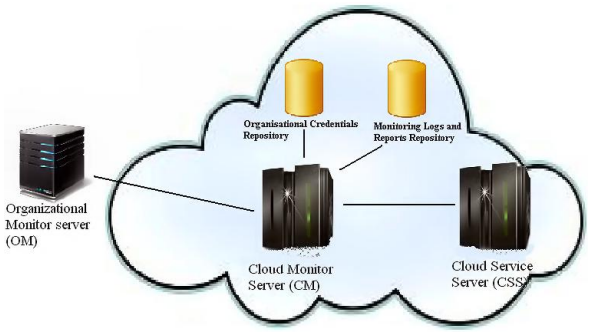


**Figure 1b: Monitoring at provider.**

The monitor will be directly connected to the cloud for making a centralized authentication for every user. Any change in user's move can be logged at the monitor before forwarded to the cloud. Same will happen from the cloud side with full synchronization [11] of the logs. The providers of cloud services will also provide access management and monitoring as a service (figure 1b) which will coordinate and communicate with the organizational monitoring server with specifically designed protocols. The overall maintenance and logs will be made at both sides in order to verify logs using digital signature technologies in order to avoid unauthorized manipulation in logs.

## 2.1 The interaction diagram of user services in Centralized MaaS.

The interaction model, following the use cases shows the sequence of interactions in form of sequence diagrams. The sequence diagrams reveal the flow of dialogues and major activities at the users and provider's level. The sequence diagrams of few activities like connecting and using service (figure 2a), verifying and flush logs (figure 2b) and log event from broker to DCMonitor (figure 2c) are important to be mentioned to give a clear picture of the whole process of monitoring.

The end users connecting to a service provider will pass through the access and monitors at both users level monitor through broker to DCMonitors as shown in figure 2a. The service is rendered by the user cloudlets [cloudsim] received by the broker and processed at data centre by holding one or more Virtual Machines (VM) depending upon the workloads, number of end users, and SLA[15]. The processing of logs will be done by the monitors at data centers or separate monitor VMs reserved for monitoring or shared VMs held by the brokers. Later in the cost analysis we will look into the cost implications with regard to both these cases. Logs that are generated synchronously at the data centre and, at the organization needs to be verified for consistency from time to time. The logs can be verified and can be flushed later on as

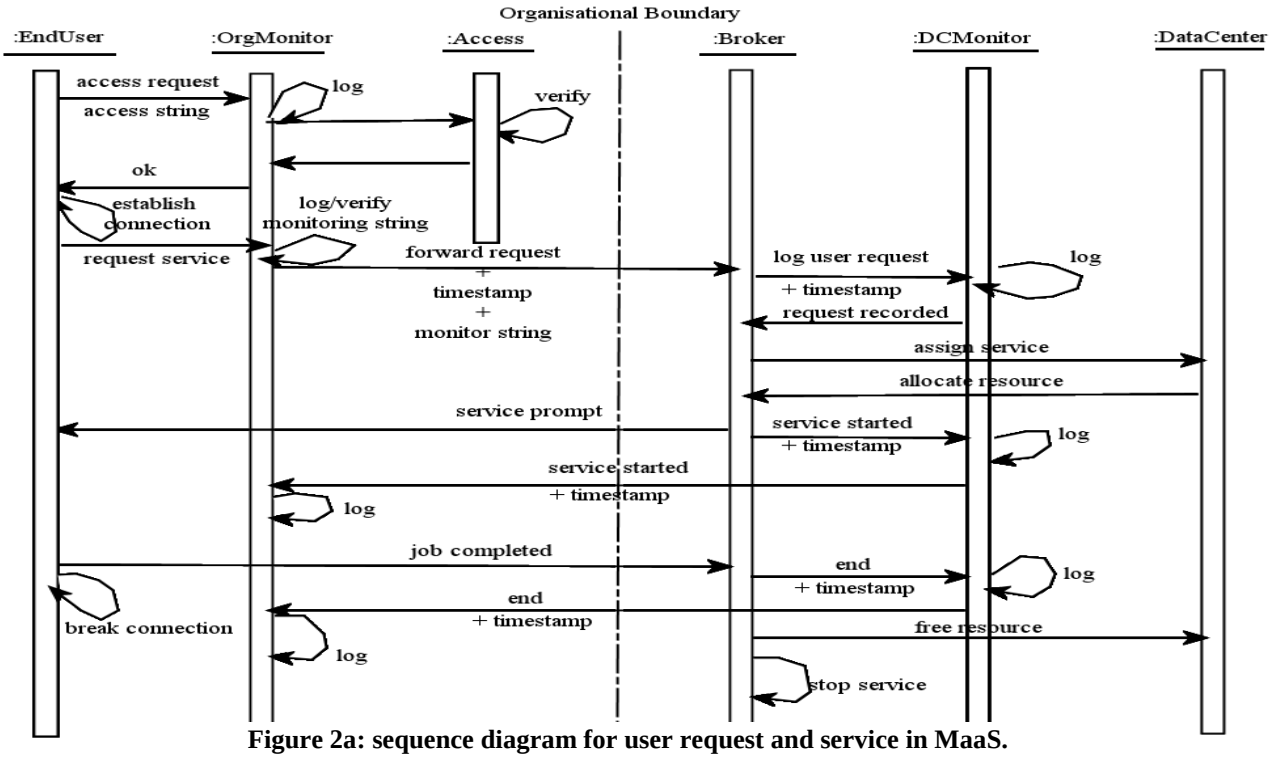


**Figure 2a: sequence diagram for user request and service in MaaS.**

shown in figure 2b. The repositories of logs can be maintained for a long time, but needs to be flushed so as to minimize storage implications. The log event will be generated by the broker based on the monitor string as shown in figure 2c. However, the processing a log and forwarding it to the user monitor for recording will also take place with consistent time stamping [8].

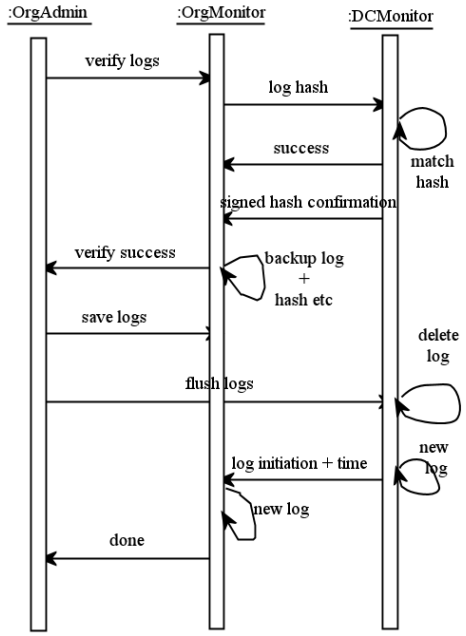


**Figure 2b: sequence diagram for verify and flush logs.**

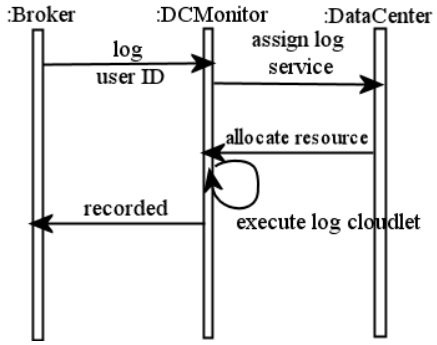


**Figure 2c: Sequence diagram for generation of log events.**

# 3. THE SIMULATION MODEL

The major concerns in having a CMaaS will be that of performance implications. Rather than looking at both the concerns together, it will be more feasible to look at them separately. The following sections will discuss the overall framework that was used by us to analyze the performance implications of CMaaS and later we have described what were the inferences.

## 3.1 The Simulation framework

The testing framework is similar to that of the basic architecture diagram shown in figure 3.

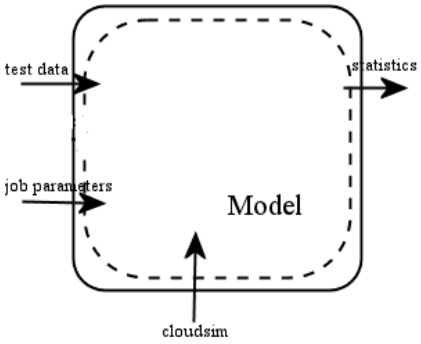


**Figure 3: Testing architecture**

The model was introduced with the job parameters which will be consisting of number of users posing requests and duration of service etc. The model output certain statistics that were analyzed and inferences were drawn. The core model was made by using cloudsim which was used to simulate the model for performance analysis. The layered cloudsim architecture [12] reveals the major layers placing Broker, Cloudlets, Virtual Machines, Cloudlet execution etc.

## 3.2 Shared vs. Dedicated VM Allocation to CMaaS.

In most of cloud architectures [14], the allocation of VM on a service is made through the brokers[12]. The brokers in CMaaS will be architecturally similar to the Cloud Service Server (figure 1b). The brokers decide upon the scheduling and allocation of resources to the user requests based on specific priorities and policies. Upon introduction of CMaaS, it becomes obvious that a policy must be incorporated whether to provide MaaS from the specially allotted VM and other resources at the datacenter or to provide MaaS on the VMs that are already allotted to the brokers specifically for the particular organization. However, in both the cases the brokers will be the center point of various monitoring activities. The complete testing will be done on two topologies that will be implemented using cloudsim. Topology 1 (figure 4a) will be the one in which the monitor will run at data centre (which is our proposed setup) and the broker will have its own set of VMs. The monitor will be running and will submit cloudlets to the separately reserved VM for a particular organization. The VMs for monitor can be internally managed or can be negotiated by the broker itself. The second topology (figure 4b) is the one where the monitoring is done at the broker's part. Here the log cloudlets will be submitted to the VMs which are allotted to the broker and will be shared by all other user cloudlets along with the log cloudlets.

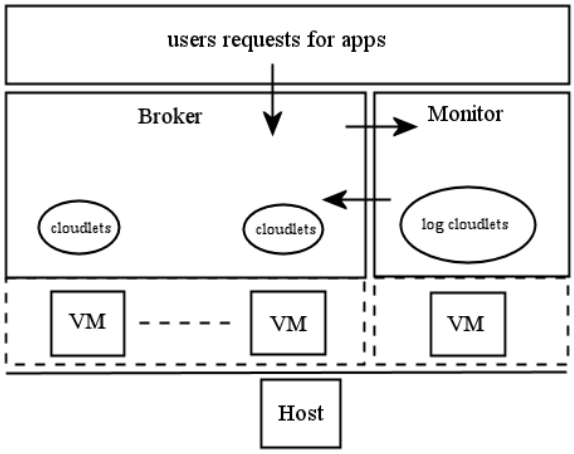


**Figure 4a: Topology1: Reserved VM for monitoring.**

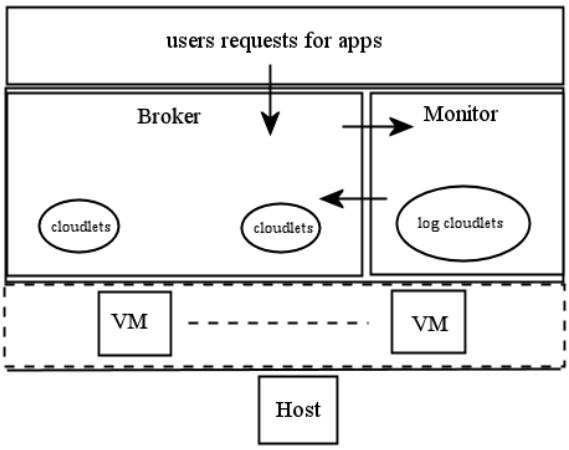


**Figure 4b:Topology2: Shared VM for monitoring.**

## 3.3 The Simulation

The simulation was done on both topology 1 and topology 2 (figure 4). The inputs in both topologies are as listed in table 1. The input length of user cloudlets, start times of each cloudlet varies uniformly [18] between 0-2000 for the former and 0 to 28800 (1 day) for each day. Also the number of users logged in per day varies from 0 to the number of users in the organization. The major reason for taking uniform distribution [18] is that, we are mostly concerned to know the overall affects of the monitoring processes on the user request processing and in case of any other empirical distributions [18] the trends might show non-natural behavior, which might lead us to wrong interpretations. The right way will be to look at a normal monthly workload of an organization and study the results. The simulation was run for three cases as given in table 1b. There were two VMs allocated to the broker and one VM for monitor (if any) at data centre. The case of no monitoring was also taken so as to compare the results to that of CMaaS for affects on user services. The basic configuration of host is also listed in table 1a.

**Table 1a: Host configurations**

| | |
|---|---|
| No of hosts | 1 |
| Dual core | 1000MIPS each |
| Linux | x86, Xen |
| RAM | 2GB |
| storage | 100000000 |
| bw | 10000 |
| Average No of Cloudlets Per user | 10 |
| Days | 30 |
| Avg no of logs per user | 10 |

**Table 1b: Test configurations**

| Topology | No of VMs at broker | Monitored? | No of VM at monitor |
|---|---|---|---|
| 1 | 2 VMs | Y | 1 VM |
| 2 | 2 VMs | Y | Shared |
| NA | 2 VMs | N | NA |

## 4. RESULTS AND INFERENCES

Simulations were made for 30 days with variable users. The figure 5 gives a clear perspective showing the per day usage of the cloud service. It gives an idea that the inputs are following realistic behavior (refer Sudden burst of network utilization in large organizations, [19]) of cloud usage in the experiment. The results incurred for 10, 20, 50, to 250 users per day follows similar behavior which forms the basis for further readings so that the usage parameters doesn't overshadow the performance investigations very much.

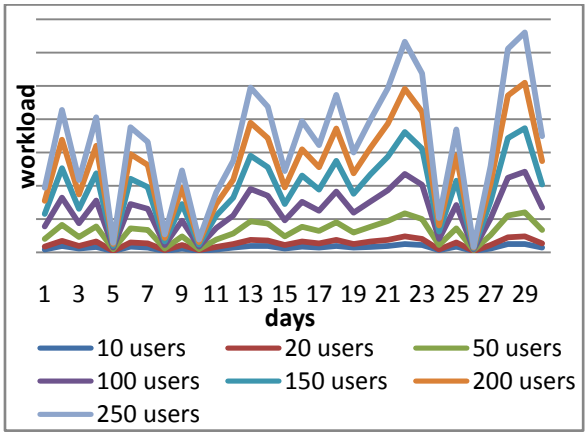


**Figure 5: Trends of usage per day used in simulation.**

Behavior of first 20 users Vs time spent at the datacenter is shown in figure 6.

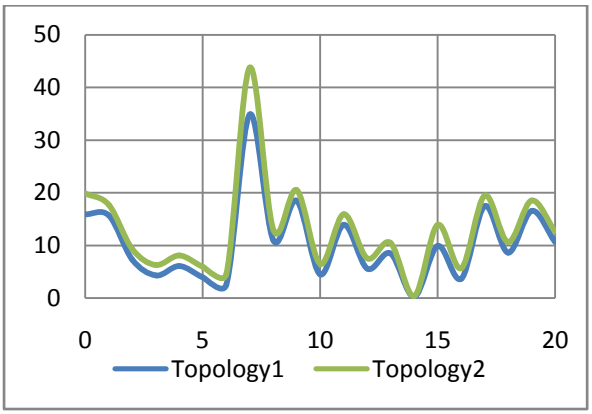


**Figure 6: Time spent by the user requests and logs at datacenter for processing**

The characteristics in case of topology1 and topology2 show very small variance. However, the topology2 requests are bound to spend more time in processing than in topology2 looking at the fact that the VMs (the major resource) is being shared by the monitor also. The major question which arises is, whether how much affected is the processing of logs with respect to the user service request processing. The case of topology2 is quite obvious (figure 7). For conformity, the readings of first 50 and last 50 logs with respect to first and last user requests were plotted (figure 7a,7b).

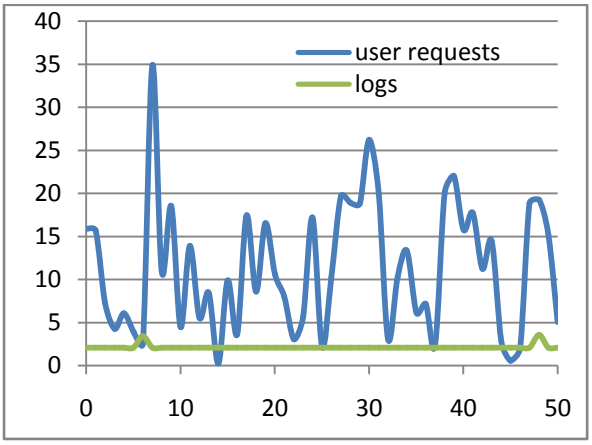


**Figure 7a: First 50 requests and logs.**

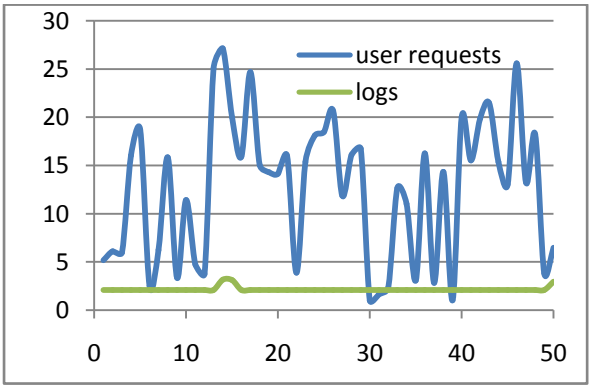


**Figure 7b: Last 50 requests and logs.**

**Figure 7: Time spent by the user requests and the logs for processing at datacenter (Topology 1).**

In case of processing logs in topology1 (which is our proposed topology) the logs are minimally affected by the overall load of the user requests. Whereas, in case of processing of logs in topology2 (figure 8a, 8b) the logs processing are affected and appear little disturbed.

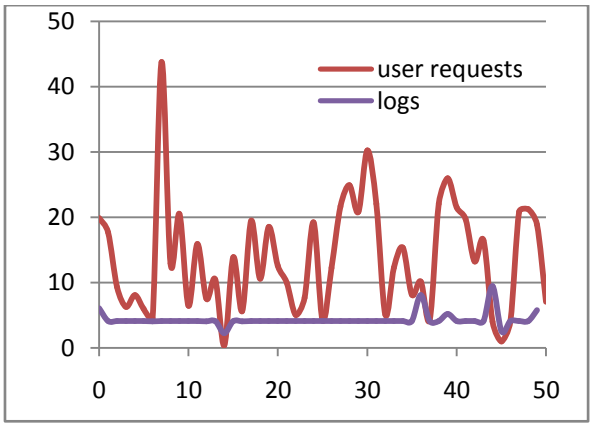


**Figure 8a: First 50 requests and logs.**

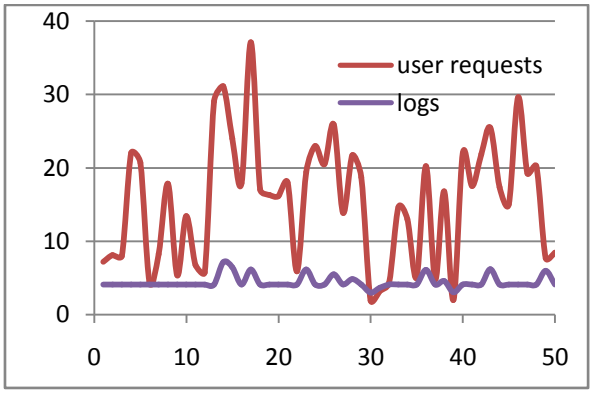


**Figure 8b: Last 50 requests and logs.**

**Figure 8: Time spent by the user requests and the logs for processing at datacenter (Topology 2).**

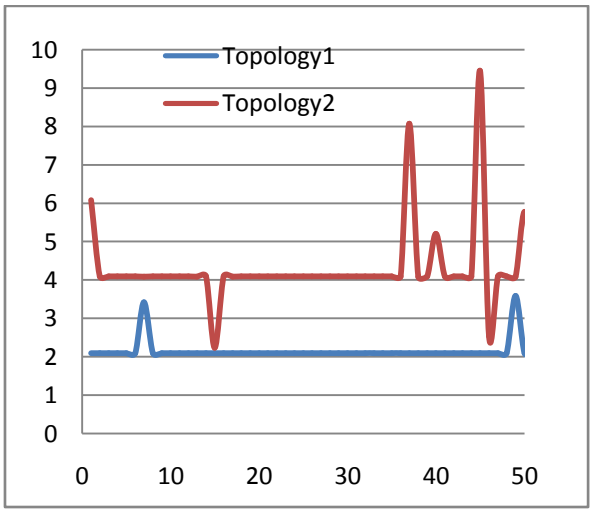


**Figure 9a: First 50 logs.**

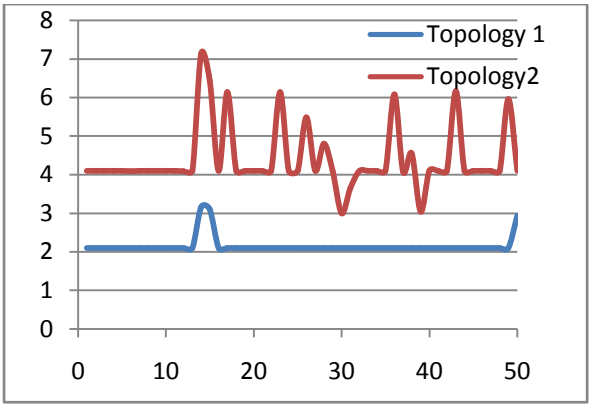


**Figure 9b: Last 50 logs.**

**Figure 9: Time spent in processing logs in topology1 and topology2.**

In many cases, time stamps of logs have to be synchronized at both Organization and DCMonitors (figure 1b). It is always good to have minimal disturbances while recording and maintaining time stamps. Observing the first and last 50 log processing in topology1 and topology2 (figure 9a, 9b), it is clear that log processing in case of topology2 appears more disturbed than that of log processing in topology1. In case of topology1, apart from almost periodic ripples there is no sign of any disturbances due to workloads. By looking at the above observations, it is obviously clear that topology1 is more suitable in terms of performance. The choice of having dedicated VMs for monitoring will always be better than that of having it on shared VMs.

## 5. CONCLUSION

In the wake of emerging need of audit ability, long term monitoring is not only advisable but, is necessary. If the monitoring is introduced, it will surely lead to some amount of extra burden on the users as well as providers in terms of performance and cost. One of the performance aspect will be to decide whether to have CMaaS on fully dedicate VMs or to have them share processing power from the allotted VMs to the service providers. As observed in the simulation results, the overall affect of monitoring on to the user processes as well as the overall affect of workloads on the monitor processing are minimal in case of dedicated VMs for monitoring. Topology1 is more promising to be proposed for long term monitoring solution. However, there is a need for doing cost analysis too on these topologies before proceeding. Thus, data centers can introduce CMaaS with fully dedicated resources (especially processing) without worrying much about performance issues.

## 6. REFERENCES

[1] Ali Khajeh-Hosseini, Ian Sommerville, Ilango Sriram, “Research Challenges for Enterprise Cloud Computing”, arXiv:1001.3257v1 [cs.DC], 2010.

[2] Jay Heiser, Mark Nicolett, “Assessing the Security Risks of Cloud Computing”, Gartner, June 2008.

[3] “Distributed Computing”, http://en.wikipedia.org/wiki/Distributed_computing, retrieved Jan 2012.

[4] Grobauer, B.; Walloschek, T.; Stocker, E.; , "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE , vol.9, no.2, pp.50-57, March-April 2011.

[5] “Guidance for Identity & Access Management V2.1”, http://www.cloudsecurityalliance.org/guidance/csaguide-dom12.pdf, 2010.

[6] Spring, J.; , "Monitoring Cloud Computing by Layer, Part 1-Part 2," Security & Privacy, IEEE , vol.9, no.2, pp.66-68, March-April 2011,doi: 10.1109/MSP.2011.33

[7] Manuel, P.D.; Thamarai Selvi, S.; Barr, M.I.A.-E.; , "Trust management system for grid and cloud resources," Advanced Computing, 2009. ICAC 2009. First International Conference on , vol., no., pp.176-181, 13-15 Dec. 2009.

[8] George Coulouris, Jean Dollimore, Tim Kindberg, Gordon Blair, “Time and Global States”, in Distributed Systems Concepts and Design, Fifth Edition, Pearson Education, chapter 14 pg 595-626.

[9] Digital Signature Standard, FIPS PUB 186-3, National Institute of Standards and Technology, http://csrc.nist.gov/publications/, June, 2009.

[10] Lynch, L., "Inside the Identity Management Game," *Internet Computing, IEEE* , vol.15, no.5, pp.78,82, Sept.-Oct. 2011 doi: 10.1109/MIC.2011.119

[11] Lindsey, W.C.; Ghazvinian, F.; Hagmann, W.C.; Dessouky, K., "Network synchronization," *Proceedings of the IEEE* , vol.73, no.10, pp.1445,1467, Oct. 1985 doi: 10.1109/PROC.1985.13317

[12] Calheiros, R. N., Ranjan, R., Beloglazov, A., De Rose, C. A. F. and Buyya, R., CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms. Software: Practice and Experience, 41: 23–50. doi: 10.1002/spe.995 2011.

[13] Ferretti, S.; Ghini, V.; Panzieri, F.; Pellegrini, M.; Turrini, E.; , "QoS–Aware Clouds," Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on , vol., no., pp.321-328, 5-10 July 2010

[14] Kirschnick, J.; Alcaraz Calero, J.M.; Wilcock, L.; Edwards, N., "Toward an architecture for the automated provisioning of cloud services," *Communications Magazine, IEEE* , vol.48, no.12, pp.124,131, December 2010, doi: 10.1109/MCOM.2010.5673082.

[15] The Service Level Agreement Zone; url: http://www.sla-zone.co.uk/; retrieved oct 2012.

[16] Ibrahim, S.; Bingsheng He; Hai Jin; , "Towards Pay-As-You-Consume Cloud Computing," Services Computing (SCC), 2011 IEEE International Conference on , vol., no., pp.370-377, 4-9 July 2011

[17] Borja Sotomayor, Rubén S. Montero, Ignacio M. Llorente, Ian Foster, Capacity Leasing in Cloud Systems using the OpenNebula Engine (2009)

[18] Jerry banks, “statistical models in simulation”,in Discrete Event System Simulation, 4/e, chapter 5, pg 129-172, Pearson Education, 2005.

[19] Andrew Odlyzko, “The low utilization and high cost of data networks”, AT&TLabs–Research, http://www.dtc.umn.edu/~odlyzko/doc/high.network.cost