A Service Level Management Authority in the Cloud

Amitay Korn, Chris Peltz, Miranda Mowbray

Abstract:

This paper introduces the notion of a Service Level Management Authority, or SLMA. An SLMA is any business entity or corporation that has a standard, independent SLM computing platform which facilitates the interaction between the Cloud vendor and the end customer. The SLMA would have an open platform allowing connection to the various management facilities exposed by the Cloud Vendor. This would include interfacing with Contracts (which for example might include Bronze, Silver, Gold and Platinum contract definitions) and monitoring agents.

External Posting Date: April 21, 2009 [Fulltext]   Approved for External Publication
Internal Posting Date: April 21, 2009 [Fulltext]

A Service Level Management Authority in the Cloud

Amitay Korn (HP TSG Software), Chris Peltz (HP TSG Software), Miranda Mowbray (HP Labs)

Abstract

This paper introduces the notion of a Service Level Management Authority, or SLMA. An SLMA is any business entity or corporation that has a standard, independent SLM computing platform which facilitates the interaction between the Cloud vendor and the end customer. The SLMA would have an open platform allowing connection to the various management facilities exposed by the Cloud Vendor. This would include interfacing with Contracts (which for example might include Bronze, Silver, Gold and Platinum contract definitions) and monitoring agents.

Problem statement

ITIL defines a Service Level Agreement (SLA) as:

> *An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers." [2]*

Traditionally, Service Level Management (SLM) systems are "owned" or driven by the customer. When Service Providers (e.g. Corporate IT or an Outsourcer) commit to SLAs, the customer should have access to the Service Level Management system, with complete transparency to SLA-related information.

Cloud computing has introduced a new set of IT management complexities. Large vendors such as Google and Amazon are very visible to the public; any system failure or blackout becomes a public issue and threatens the broader adoption of Cloud Computing. To address these issues, Cloud vendors must improve their uptime and their resilience. More importantly, they must become more transparent in how they work with customers during times of failure, including handling credits when SLA breaches occur. For example, Amazon.com's S3 service has a SLA offering a 10-15% percentage discount on the next month's bill to customers experiencing more than 0.1% service downtime in a month. But the burden of monitoring SLA compliance is left to the customer, and customers have to actively claim their discounts, presenting proof of the SLA breach to Amazon.

Customers may not be happy with having the whole Service Level monitoring and management system owned by a Cloud Vendor such as Amazon S3, but would prefer not to have to carry out this work themselves. We believe that *there will be an increased demand to have SLAs that are monitored and managed by an objective third party*. The intent of this paper is to introduce the concept of a third party Service Level Management Authority, along with the opportunity for HP to differentiate itself in this management of cloud-based services.

Our solution

The solution introduces the notion of a Service Level Management Authority, or SLMA. An SLMA would be any business entity or corporation that has a standard, independent, SLM computing platform which facilitates the interaction between a Cloud vendor and the end customer. This solution assumes there are a limited number of cloud vendors but a significant number of corporations consuming the cloud services offered from these select vendors.

There are some important components of our SLMA solution. All SLMAs must have capabilities to monitor both performance and availability of cloud services in terms which the customer understands. The SLMA would have an open platform allowing connection to the various management facilities exposed by the Cloud Vendor. This would include interfacing with Contracts (which for example might include Bronze, Silver, Gold and Platinum contract definitions) and monitoring agents. At the same time, the Cloud vendor would need to open their infrastructure by adding entry points for customers to select their SLMA of choice (i.e., it must be assumed that customers will have a choice of SLMAs). Vendors will also need to open their billing systems to accept credit chargeback requests from the SLMA on behalf of specific customers. The network topology and proposed architecture is shown in the figure below:
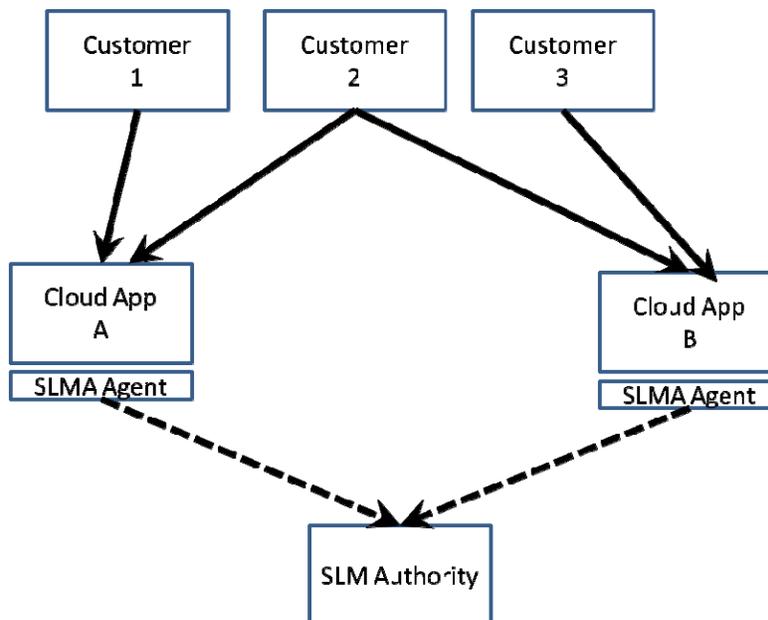
Topology for Configuration of SLM Authority, Cloud Vendor, and Customer

In our approach, it is important to point out that the role of Enterprise IT is not eliminated, but it must evolve. In particular, we see that IT will need to take on the following responsibilities in this type of environment:

1. IT must educate the business on the cloud-based services available for use
2. If an SLA has been breached, IT must claim the appropriate credit from the cloud provider
3. There will be a strong desire to integrate cloud SLM with internal IT management systems
4. All participants, including IT, will want a standardized, simplified service contract interface

On the third point, it is essential that this solution has to respect the complexities of intra-corporate Service Level Management. We therefore envisage a set of solution offerings each priced to target different markets segments:

1. **Synthetic Monitoring**, focused on monitoring at the Cloud vendor level only. The SLMA will record contractual violations only when the Cloud service is fully down and unavailable.
2. **Customer Monitoring**, where monitoring is done at the customer instance level. This solution will give a more complete measure of the Cloud environment from the customer perspective.
3. **Transaction-based Monitoring**, which might leverage technology such as HP Business Availability Center. It is assumed that this option is costly and required a certain level of customer maturity.

The general recommendation is for customers to first implement customer-level monitoring (which would include synthetic-based monitoring). A second natural step would be consideration of a transaction-based approach to Service-Level Management.

Evidence the solution works

The solution involves the use of existing HP Software technology to address the Service Level Management requirements. HP Software currently offers a SLM module in HP Business Availability Center (BAC). BAC SLM is a high-end solution focused primarily on monitoring business transactions. HP BAC Real User Monitoring (RUM) product is used to measure performance and availability. This is combined with our HP Software-as-a-Service offerings which enable cloud-based access to management information.
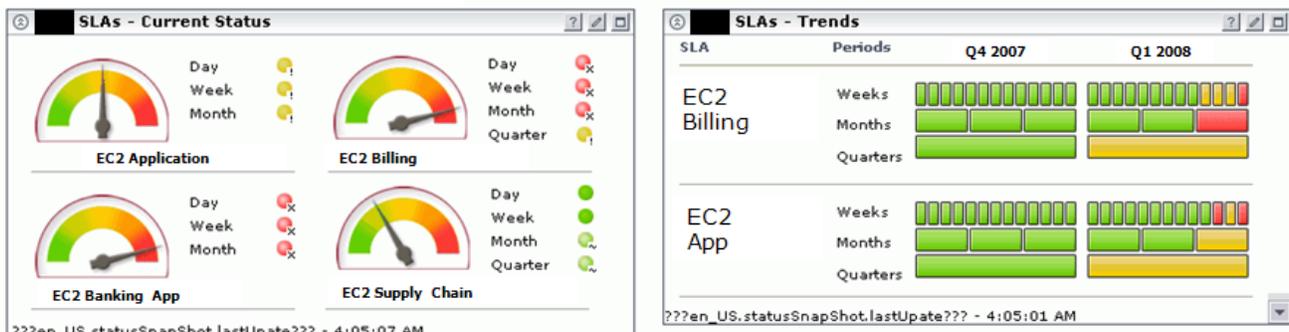
The following use case illustrates the solution concept further:

> *Acme Inc. purchases the Amazon EC2 service and requires some level of SLM. Amazon suggests to Acme 2-3 independent, objective SLM audit services, one of which is from HP. Each of these audit services already integrates with customized Amazon EC2 contracts. If HP is the chosen SLMA, Business Availability Center Real User Monitoring (BAC RUM) agents would be installed at locations that are relevant to the customer. Both the Client and Amazon EC2 have web-based access to the SLM data on HP SaaS servers.*

Competitive approaches

There are significant differences between the requirements for standard solutions such as BAC SLM and the solution presented here:

- An SLMA will have to deal with scale and complexity issues given the IT relationships
- The pricing model for an SLMA must be very low; it should not reach above 10% of the total deal size.
- SLMA is a Cloud Computing service, although not necessarily paid for by direct subscription.
- A billing component is a natural part of the SLMA offering.

There are also competitive approaches by other companies. Hyperic is an open source monitoring and management software company. They launched a CloudStatus service in June 2008 which monitors Amazon Services, and plan to extend their monitoring services to Google App Engine and other sites [4]. CloudStatus just monitors Cloud Vendors from the outside; unlike our proposal here, it does not offer an SLMA. We are not aware of any competitors that have a business plan for offering an SLMA.

Next steps

Development work is underway to prototype this solution using HP BAC and our Software as a Service offerings. One interesting application of this solution is delivering a customer-focused health status. For example, communication or network problems may have the effect that the Cloud service works perfectly as measured by the SLMA, but, from the end user's perspective, the "system is down". The SLMA capability outlined in this paper could be extended to also handle client-based monitors which help with diagnosis in such cases.

References

[1] Koman, R. 2008. Gmail Outage Raises Doubts About Cloud Computing. *NewsFactor Network* (http://www.newsfactor.com/story.xhtml?story_id=61274)

[2] OGC 2007. *Official Introduction to the ITIL Service Lifecycle*. Stationary Office Books.

[3] Schiffman, B. 2008. Customers Shrug Off S3 Service Failure. *Wired Blog Network* (http://blog.wired.com/business/2008/02/customers-shrug.html)

[4] Shankland, S. 2008. Can you trust your business to Google's cloud? *CNET News – Digital Media* (http://news.cnet.com/8301-1023_3-9989019-93.html)