A Multi-Agent Based Approach to Monitoring IaaS Security SLA

Jiajin Cao[1,2,a], Chunhe Xia[1,2,b] and Xiaochen Liu[1,2,c]

[1] Beijing Key Laboratory of Network Technology, China

[2] School of Computer Science and Engineering, Beihang University

[a]cdoublej@126.com, [b]buaaxch@126.com, [c]ann4498@sina.com

Keywords: Cloud Security, IaaS, Security SLA, SLA Monitoring.

Abstract. Security SLA in cloud service is of great importance for user confidence, but there is little research on it. In this paper, we analyze the important security requirements in IaaS cloud, bring up a native scalable monitoring framework for security SLA in IaaS cloud and raise monitoring methods for important security SLAs in the OpenStack platform. The monitoring framework raised in this paper provides high scalability because of the RESTful design, and has a universal suitability.

Introduction

Security is a big concern for enterprise to use cloud platform and there has been a lot of work concentrating on it. Service Level Agreement defines the important metrics for the service provided to the customers. Security SLA is very important for increasing user confidence but there is little literature researching in it.

Firstly, we classify the SLAs into two categories, which are performance SLAs and security SLAs, and research into the security requirements in IaaS cloud platform and then put forward the important security SLA metrics. Then we introduce the framework of our monitoring approach and the functions of each component in the framework. Finally we analyze the characteristics of security SLA metrics and list our detailed monitoring methods on the platform of OpenStack.

Related Works

With the rapid development of Cloud computing and the growing scale of cloud platform, the need for monitoring of Cloud computing platform and SLA has also been increasing. For the moment, there have been many works on the Cloud computing platform and SLA monitoring area.

Authors in [1]presented an overview of QoS monitoring approach. The prototype system they presented instrumented the SOAP engine library with logging statement to emit the information for QoS measurement. Besides, other techniques such as low-level sniffing and proxy-based solutions were also discussed in their paper.

In [2], the authors implemented a conceptual network monitoring framework entitled CloudCop using SNMP. CloudCop adopts Service Oriented Enterprise model, and it's framework consists of three components: Backend Network Monitoring Application, Agent with Web Service Clients and Web Service Oriented Enterprise.

Emeakaroha et al. [3] presented the LoM2HiS framework for the mapping of low-level resource metrics to high-level SLA parameters. It mainly includes a runtime monitor continuously monitoring the customer's application status and performance; then in [4] they proposed Cloud Application SLA Violation Detection architecture (CASViD).

CSLA [5] is a WSLA [6] based SLA model for Cloud services. The model provides agents to handle customer requirements and mapping them into aggregated SLA document. After the SLA aggregation and service provision, the CSLA model provides means to measure performance, evaluate SLA and bill. The drawback of CSLA model is that it did not consider the dynamic nature of SLAs in Cloud environments.

Chau et al. [7] present an event-based SLA monitoring approach as part of the eQoSystem project. In the SLA model, SLAs consists of multiple SLOs and use various metrics to indicate different measurements. In contrast to that, our QoS events focus on the performance and status level. Furthermore, we additionally address how security QoS attributes can be monitored from server side.

Monitoring Approach

Motivation Scenario. Fig. 1 shows a typical security concerned IaaS cloud scenario. An IaaS cloud platform contains physical resources like hosts, routers, storage devices and security devices. Physical resources can be virtualized to form a resource pool, and with some resources management engine, they can be allocated to users on demand, often in the form of virtual machines. The user need to acquire a real-time access to the status of computing resource usage, such as the cpu, memory percentages, and other metrics like storage usage and bandwidth. At the same time, the user need that other people have no access to the source data virtual machine but the specified virtual machines, therefore, all the virtual machines communicate with each other in a secured tunnel.

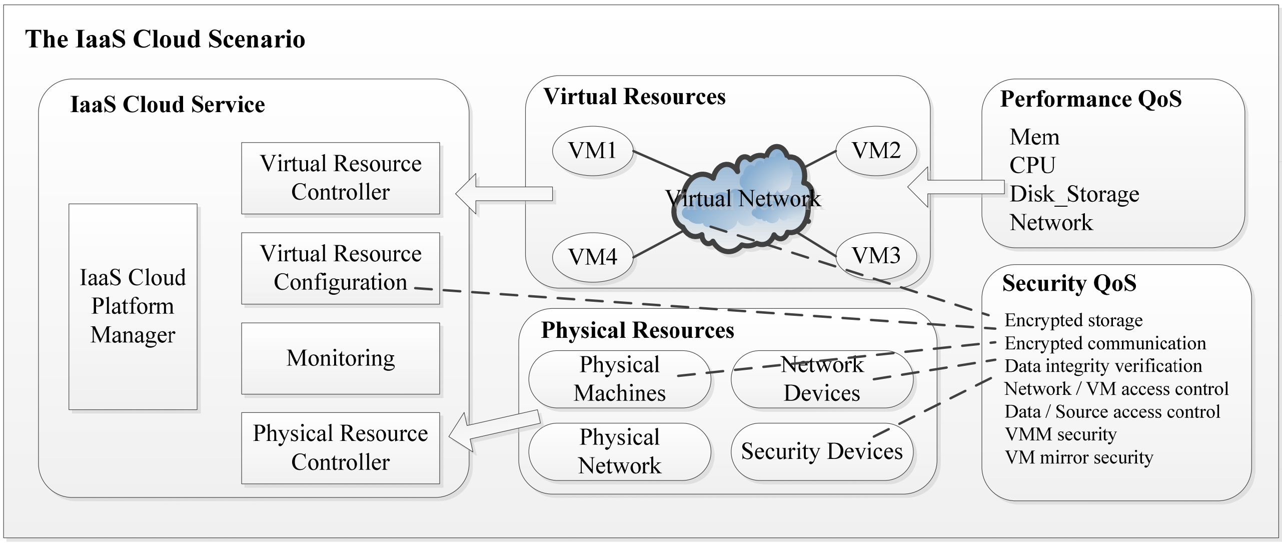

Fig. 1 A typical security concerned IaaS cloud scenario

To satisfy the need of the user in the scenario above, accurate and fine-grained resource monitoring activities, especially for the security demand, is required. This paper provides an approach for monitoring the security demand in IaaS cloud platform.

Monitoring Framework. As mentioned in Introduction section, in this paper we propose, develop and validate a novel approach for SLA monitoring in the IaaS cloud environments. Our approach include mechanisms for efficient cloud monitoring for both performance and security SLAs and provides standard interfaces and communication protocols that enable cloud service providers and users to gain awareness of the whole status of the system and service in the format of the SLO metrics. The framework comprises three main components namely, Monitoring Manager， Monitoring Agent and SLA Analyser.

The Monitoring Manager is the interface of the whole monitoring system, it receives SLA document, divides and converts the SLA elements into detailed monitoring requirements, distributes the requires to the specified Monitoring Agent, and provides the view of the monitoring result for the cloud service providers and users; The Monitoring Agents resides on both the virtual machines and physical machines as they need all aspects of information about the IaaS cloud platform. They collect specific information from the hosts according to the requirements published by the Monitoring Manager and send the collected data to SLA Analyser. The SLA Analyser are responsible for the storage and analysis of the aggregated monitoring data, it takes on the data from the Monitoring Agents and store them in a distributed database Mongo DB, and fetch the relevant metrics for the SLA from the data to form the SLA analysis documents and submit it to the Monitoring Manager for user view.

Monitoring Strategy

As mentioned in the Introduction section, this paper focuses on security SLA monitoring. In this section, we will introduce the monitoring strategy adopted in our approach, including the important SLA metrics in IaaS cloud, data and log file that we need to acquire for monitoring these metrics, and the analyzing and mapping method for the data and SLA metrics.

Important SLA Metrics. Based on the properties of SLA, we divide them into two categories, performance SLA and security SLA. The performance SLA indicates the important parameters that describe the ability of the resources and the status of the infrastructure service. We list the most important parameters in cloud as an infrastructure service.

Table 1. Performance SLAs for IaaS

Parameter	*Description*
CPU capacity	CPU speed for VM
CPU utilization	CPU usage percent
Memory size	Cash memory size for VM
Memory utilization	Memory usage percent
Boot time	Time for VM to be ready for use
Storage	Storage size of data for short or long term of contract
Availability	Uptime of service in specific time
Bandwidth	Network speed for VM

The security SLA indicates the security requirements in the cloud of infrastructure service. We analyze the SLA metrics in the respects of Confidentiality, data integrity, access control and the security requiments of the virtual machine, as shown in Table 2.

Table 2. Security SLAs for IaaS

Respects	*SLA Metrics*
Confidentiality	Encrypted storage
	Encrypted communication
Data Integrity	Data integrity verification
Access Control	Network / VM access control
	Data / Source access control
VM Security Requirements	Virtual Machine Manager security
	VM mirror security

Detailed Monitoring Methods. Considering the different source and data type of the SLAs above, different monitoring methods are raised. Some monitoring system get the target data from the statistical information provided by the virtual machine manager, but these data are not accurate because the VMM introduces deviation brought by the virtualization. In order to improve the accuracy of the monitoring data, we deploy a monitoring agent in the VM to be responsible for collecting the performance data from the VM itself. The Table 3 below shows how the monitoring agent collects the specific metrics.

Table 3. Monitoring methods for performance SLAs

Performance SLAs	*Monitoring Methods*
CPU capacity	Judge the os from sys.platform, if linux: the ‘model name’ in /proc/cpuinfo; if win: wmi.WMI().Win32_Processor().
CPU utilization	psutil.cpu_percent().
Memory size	psutil.virtual_memory()[‘total’].
Memory utilization	psutil.virtual_memory()[‘percent’].
Storage	Go through the iterator psutil.disk_partitions(), for each of them, sum up psutil.disk_usage(path)[‘total’].
Bandwidth	Caculate psutil.net_io_counters()[‘bytes_recv’] every second, the max increment is the bandwidth.
Boot time	The time between ‘Starting instance’ and ‘released * _locked_do_build_and_run_instance’ in the VMM log file /var/log/nova/nova-compute in the host.

The security SLAs are not reflected inside the VM but distributed in configuration, data storage, network communication, so we need to collect data from all parts of the IaaS cloud platform, including compute node, network node and even the network components. Besides, there is a large volume of the source data for security SLAs, so we specify the SLA requirements when the monitoring agent startups to enable it collect and transfer the specific data thus reducing the network burden. The Table 4 shows the specific monitoring methods for each aspects of security SLAs.

Table 4. Monitoring methods for security SLAs

Security SLAs	*Monitoring Methods*
Encrypted storage	Judge the Volume Type of the disk attached to the VM.
Encrypted communication	Connect to the OVS bridge and use tcpdump command to check the connection flag, judge whether it's encrypted.
Data integrity verification	Remote data integrity validation and integrity checking challenge to the storage node, check the correctness of the returned code to determine the integrity of the data.
Network / VM access control	Match the SLA to rows in the iptables of the virtual networking device and check the correctness.
Data / Source access control	Extract the user-role-project info from the keystone component and obtain the privilege of role from the configuration, finally compare them to the SLA
Virtual Machine Manager security	Maintain a knowledge base of the vulnerability of VMMs and Check the operating VMM version.
VM mirror security	Raise an instance, install a secure software and run the security check, and judge the safety according to the check log.

After the monitoring agents obtain the specific data, they push the data to the SLA Analyzer for further analysis.

Conclusion

The main contribution in this paper comprise 3 parts. 1) Security SLA requirements in IaaS cloud are analyzed and important security SLA metrics are summed up.2) A native monitoring framework for performance and security SLAs with multi-agents and little network burden are brought up.3) Effective monitoring methods for import security SLA metrics on OpenStack platform are raised.

Acknowledgements

This work was financially supported by the National Natural Science Foundation of China (Grant No.61170295) and the Joint Funds of the National Natural Science Foundation of China.

References

[1]N. Thio and S. Karunasekera, Automatic measurement of a QoS metric for Web service recommendation. (2005)

[2]Mydhili K. Nair and V. Gopalakrishna. ‘CloudCop’: Putting network-admin on cloud nine towards Cloud Computing for Network Monitoring. IEEE International Conference on Internet Multimedia Services Architecture and Applications, (2010)

[3]V. C. Emeakaroha, I. Brandic, M. Maurer and S. Dustdar. Low level Metrics to High level SLAs - LoM2HiS framework: Bridging the gap between monitored metrics and SLA parameters in cloud environments. International Conference on High PERFORMANCE Computing and Simulation, (2010)

[4]Vincent C. Emeakaroha, Tiago C. Ferreto, Marco. A. S. Netto, Ivona Brandic and Cesar A. F. De Rose, CASViD: Application Level Monitoring for SLA Violation Detection in Clouds. 42, 12(2012)

[5]Guihua Nie, E. Xueni and Donglin Chen, Research on Service Level Agreement in Cloud Computing, (2012)

[6]Alexander Keller and Heiko Ludwig, The WSLA Framework: Specifying and Monitoring Service Level Agreements for Web Services. Journal of Network & Systems Management. 11, 1(2003)

[7]Tony Chau, Vinod Muthusamy, Hans Arno Jacobsen, Elena Litani, Allen Chan and Phil Coulthard. Automating SLA modeling. Conference of the Centre for Advanced Studies on Collaborative Research, October 27-30, 2008, Richmond Hill, Ontario, Canada, (2008)