Journal of Theoretical and Applied Information Technology
30th June 2012. Vol. 40 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CLOUD MONITORING BASED ON SNMP

[1]J. SWARNA, [2]C. SENTHIL RAJA, [3]DR.K.S.RAVICHANDRAN

[1,3]SASTRA University, Thanjavur, Tamil Nadu, India

[2]Alcatel-Lucent India Limited, Chennai, India

Email: [1]swarna.jp@gmail.com

ABSTRACT

With the new trend in the industry being everyone playing the role of a cloud player, lots of pressure has been mounted on them as to how the resources are efficiently managed, thus providing elasticity to the end-user's demands. When coming to a networked environment with larger hosts, especially in a cloud environment, the monitoring tool should well be capable of handling the load and reproduce the results in quicktime. In lots of cases SNMP based monitoring proves worthy of the effort being put irrespective of the size of the environment. Using SNMP MIBs may prove to be an effective approach for dealing with the underlying information of different hosts in a cloud environment. The monitoring tool is also capable of dealing with the SNMP checks.

Keywords: *Cloud Monitoring, SNMP Mibs, Management, Cloud Environment, Oids, Discovery, Auto-Registration*

1. INTRODUCTION

Cloud Computing is the delivery of computing as a service rather than as a product, whereby shared resources, software and information are provided to computers and devices as a metered service over a network. The end-users are metered or charged[11] based on their usage. Even before providing the resource to the end-user they have to prepare a legal document which they call Service Level Agreement (SLA) which contains all the information regarding the lending. Even though they may strictly follow their SLAs, still they have to effectively manage the resources they promise to offer, so as to beat the competition in the market among the other players. Though, many monitoring tools are available all are not expected to perform every other feature.

In a large environment like cloud, the vast pool of resources have to be added to the existing networked resources. This helps in the increasing elasticity of the cloud and to meet the end-user requirement in less time. A monitoring tool with the auto-discovery feature is widely accepted in this scenario. When connected in a networked environment normally the hosts are to be added one by one. Starting with the IP address, different parameters in both the monitoring host or the server and the monitored host or the agent has to be matched upon. Sometimes this has to be set for each individual hosts in each platform separately. Also this requires the hosts be connected to the network.

With auto-discovery this is made easy by server automatically detecting the hosts when connected in a networked environment. Also the monitoring tool deals with the SNMP based monitoring of hosts[12], our work is made easy in that SNMP MIBs are used to query about the status of the host in a cloud. These MIBs access the base information of the hosts as well as communicating with the server.

2. OVERVIEW

In an environment where all the devices are networked in order to connect each other, monitoring of such systems plays a vital role in effective management of devices. In terms of resources utilization, memory or disk available, network monitoring plays a great part. For monitoring, some electronic devices have also been designed and installed for large-scale distributed systems.

Journal of Theoretical and Applied Information Technology
30th June 2012. Vol. 40 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

These devices just include the sensing capabilities for online measurement, actuators for controlling certain variables, microprocessors for processing the collected information and making decisions based on the algorithms defined for them, and some communicating device to exchange information. Such devices are called networked intelligent agent monitoring system. Such systems usually generate a huge amount of spatial-temporal data while monitoring. Based on those algorithms, the desired information is fetched while the rest of the data are discarded after a certain period.

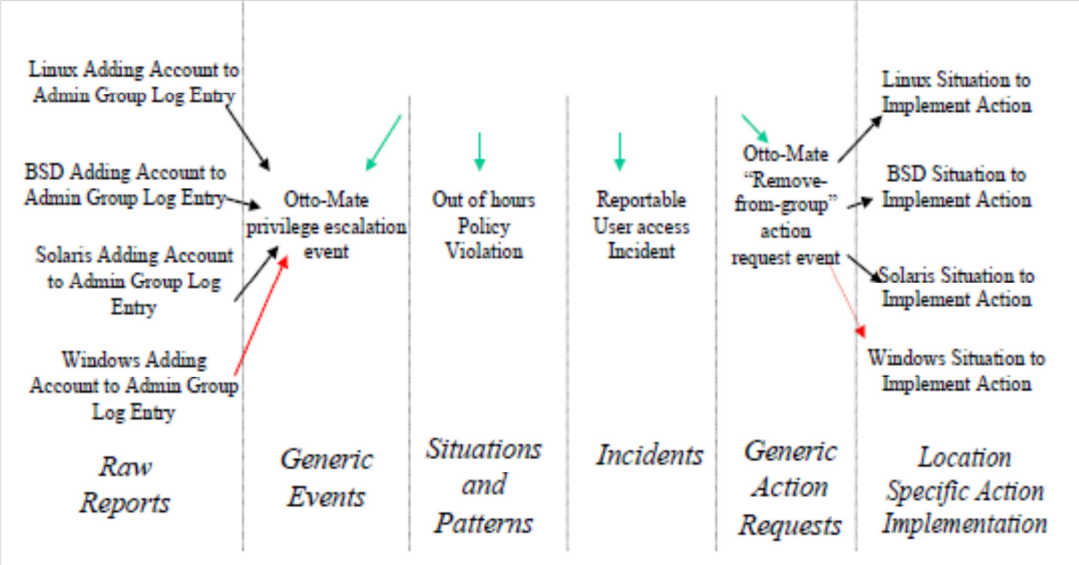

Figure 1: Normalizing Events and Requests

Another distributed reasoning system called Otte-Mate[4] is used to detect, reason out and respond to abnormalities in the monitored network. Some information might relate to the system, some might be network related, some might be resource-specific and there will be events associated with each incident.

By distributing the reasoner agents and installed them on distributed resources with the distributed parallel algorithms they are able to monitor the event patterns. Distributing the reasoning makes the system extremely resilient. Moreover the agent may discard those events which do not meet the reasoner's threshold are discarded after a certain time period. This helps to reduce the load which normally come in the centralized system.

In the case of a grid environmemt there has been massive deployments of devices from multiple vendors. However, there has to be a way for communication among them through several protocols and network topologies. Network monitoring in this context takes care of the service configurations, data measurements and network availability. There the data ontology definitions[3] and rule engines are used for reasoning out the parameters.

3. CLOUD MONITORING ON SNMP

In the process of managing and monitoring network performance, solving the network problems and planning for the network growth, SNMP came in handy for the network administrators. Other protocols such as CIM/WMI[2] also provide information representation and management, they are about to perform low-level functionalities. Further the script based on the metric definitions is to be followed in order to make them perform high-level operations.

However, SNMP is an open protocol and for years it has been the standard protocol used between network management systems and network elements. With the appropriate SNMP package installed for a given platform we can easily import the MIB's, poll OID's and manage SNMP-enabled devices. When the monitoring area becomes large it is possible that there are as many security threats as possible. With the SNMPV3 protocol in place, authentication of the node or anyone requesting the management information is made mandatory. Also

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

by giving access-permissions on the identifiers we can limit their access to any third parties.

All the data centres and the cluster nodes as well as each node in the network forms a cloud monitoring environment. The standard and custom monitoring of applications in cloud involves a number of simple checks in order to get more information. However the number of information gathered through MIBs is dependent on those MIBs installed on the system.

3.1. CLOUD MONITORING

The type of cloud may it be a private, public or a hybrid one, the fundamentals of monitoring and systems management are the same. The applications installed in them or the operations being performed must have unified visibility, even though they may be distributed, they should be made aware of the cloud infrastructure. Dynamic resource prioritization means that cloud servers come and go and change constantly. So enabling of multiple monitoring solutions for this kind of environment may be a chaos or is not advisable.

In order to ensure availability and maintenance of service levels pertaining to critical infrastructure those structures have to be constantly monitored in addition to the traditional data centres. Even with all those available resources sometimes the spell fell on the availability of a particular resource. The availability of a resource is governed by a number of algorithms running in the cluster node as well as many other data centres to ensure the availability at a particular place within a given region. They also determine the number of copies to be maintained. Lower number of copies may result in latency while the end-user is fetching the resources. These latencies are to be computed by counting the number of requests coming from a particular region and the number of copies available at that instant to cater the need.

3.2. SNMP MIBS

The advantage of SNMP is the type of data that can be acquired from the system. [1]The SNMP agents provide essential information for effective monitoring and troubleshooting of the network. For example, when using a protocol analyser to monitor network traffic from a switch's SPAN or mirror port, physical layer errors are not shown. Neither the switches forward the error packets to either the original destination port or to the analysis port. But the switch maintains a count of the discarded error frames and this count can be retrieved using a SNMP query.

We can easily set the properties defined for monitoring using a command line or a configuration file. Properties specified on the command line override the properties in the configuration file. SNMP exposes management data in the form of variables on the managed systems, which can then be queried by managing applications.

However SNMP does not define which information a managed system should offer. The SNMP uses an extensible design, where the information for managing the system is designed by Management Information Bases (MIBs)[9]. These describe the structure of management data. They use a hierarchical namespace called Object Identifiers (OIDs). Each OID is associated with a variable. MIBs use the notation defined by ASN.1.

3.2.1.MIBPARSER

MibParser is used to parse the MIBs and fetch the respective OIDs from their systems. They also perform the ping and trace functions. However they are allowed access only to the default MIBs or the one s which are extended. In order to extend the custom MIBs , we need to create a subagent. This subagent can be separately compiled and included[17] to the net-snmp package via agentX functionality.

The comunication between the actual net-snmp agent and the subagent is through the master-agent communication. The subagent is registered along with the net-snmp agent. The MibParser helps to parse through the MIB identifiers. By converting a textual string into a numeric identifier or vice versa, this helps to analyse the MIBs used in the particular system.

3.3. NETWORK MONITORING – AUTODISCOVERY OF HOSTS

The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages. It is one of those functions involved in network management. The intrusion detection[10] system monitors the network for defects causing from outside while a network monitoring system

Journal of Theoretical and Applied Information Technology
30th June 2012. Vol. 40 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

monitors a network for problems being caused by the overloaded servers, network connections and other devices.

Commonly measured metrics are response time, availability, uptime, CPU usage, memory and disk usage though both consistency and reliability are starting to gain popularity. In order to monitor those metrics consistently, the host be added to the monitoring system initially. This normally involves setting up the configuration necessary for connecting to the server. However this process is time-consuming and it leads to increasing overhead with the increase in the number of hosts in the network.

Imagine the network of a cloud, and in a time, the cloud may expand or contract as many times as possible. In that scenario the manual entering and deleting of each host may not be favoured as it is almost a task which can be automated. The monitoring tools like zabbix provide automatic discovery[14] of the hosts to be monitored in the network. And because of this feature hosts are added in the network in no time based on the discovery rules common to all other hosts.

The monitoring tool being an SNMP based one can query the host using the SNMP MIBs. Upon adding the hosts we can define certain actions on the group of hosts. Upon discovery, the hosts are added to the respective host groups based on the operations [14] defined. On each host groups certain actions can be implemented by defining the actions.

When a previously unknown host enters a network asking for an agent check, that host is registered with the server of the monitoring system. After which the host is added to the system for monitoring without actually deploying[15] any agents in them. This is very handy in the picture of a wide cloud scenario.

4. IMPLEMENTATION

This section presents the implementation of our proposed cloud monitoring setup based on SNMP. The major components needed for implementation are the NMS i.e. Zabbix, MibParser and AgentX. Here Apache is the web server being used and the web frontends of the interface are powered by PHP.

MibParser is used to parse through the MIBs. In the net-snmp agent configuration file the sub-agent can be extended with the following line.

master agentx

Once the agent is started, the custom MIBs are assigned the system's current values are accessible to the authenticated person. We perform the actions based on zabbix agent's system name, CPU load on the discovered hosts. That is, the new host coming into the network is performed these two actions and added into the corresponding host groups.

Monitored host	Uptime/Downtime	SNMPv2 agent: .1.3.6.1.4.1.6527.3.1.2.1.1.1.0	SNMPv2 agent: UCD-SNMP-MIB::laLoad.1	Zabbix agent: system.uname
Redhat 4	20:21:41			
-	16:26:30			
win718	20:21:15			
win719	20:21:15			
Redhat 20	20:21:15			

Figure 2: Discovered hosts based on Discovery Rules

Journal of Theoretical and Applied Information Technology
30th June 2012. Vol. 40 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The table headings show the monitored hosts, their uptime/downtime, OIDs of the MIBs as well as the zabbix agent system name. These OIDs and the system name are called the discovery rules to be performed when a host enters a network, thereby making the host discovered.

Upon adding the hosts further operations like adding to a host group and Linking to Template are performed

.

ACTIONS Even

Displaying 1 to 3 of 3 found

Name	Conditions	Operations
Auto Discovery- Linux Servers	Uptime/Downtime >= "30" Discovery status = "Discovered" Service type = "SNMPv2 agent" Service type = "Zabbix agent" Host IP = "10.91.1.1-255"	Link to template "Template_Linux" Link to template "Template_SNMPv2_Device" Add to group "Linux servers"
Auto discovery. Linux servers.	Received value like "Linux" Discovery status = "Up" Service type = "Zabbix agent"	Link to template "Template_Linux" Add to group "Linux servers"
Auto discovery. Windows servers.	Received value like "Windows" Discovery status = "Up" Service type = "Zabbix agent"	Link to template "Template_Windows" Add to group "Windows servers"

Figure 3: Host Groups added with conditions and operations

This is how the discovered hosts are categorised and added to the monitoring system as we normally do for monitoring with agents. The whole objective of this issue is to add the hosts into monitoring as much as possible in less time without the overhead of manipulating each and every host.

5. CONCLUSION

Currently many monitoring tools are available on the market for monitoring the resources. And with the trend wherein every other vendor assuming the role of a cloud player, we can expect cloud's presence predominant in the network. In order to ease the monitoring we are opting for a well-used protocol in TCP/IP networks called SNMP. With SNMP enabled in every device inherently we can easily monitor the host when it enters into the monitored network. By separating default MIBs from the custom MIBs they ensure the security of the system by providing what is allowable to the common user and hidden from them. Extending the custom MIBs is through the AgentX functionality. The auto-discovery and the auto-registration features of the NMS registers the host when it enters a network. The extension of this capability of monitoring the network by an SNMP-based NMS is to extend the same to a broader cloud-scenario without compromising the functioning and overhead. The future work also includes extended agent functionality apart from the inherent SNMP service available to all hosts efficiently.

REFERENCES

[1]Ya-Shiang Peng and Yen-Cheng Chen, "SNMP-Based Monitoring of Heterogeneous Virtual Infrastructure in Clouds",

[2]Weidong Min, "Distributed network resources monitoring based on multi-agent and matrix grammar" Fourth International Symposium on Parallel Architectures, Algorithms and Programming, 2011

[3]Md Tanzim Khorshed et al, "Monitoring insiders activity in cloud computing using rule based learning", International Joint Conference of IEEE Trustcom-11, 2011

[4]S.Musman, " Using parallel distributed reasoning for monitoring computing networks", The 2010 Military Communications Conference- Unclassified Program- Cyber security and Network Management.

[5]http://technet.microsoft.com/en-us/library/cc776379(v=ws.10).aspx

[6]http://www.zenoss.com/solution/cloud-monitoring

[7]http://www.zabbix.com/wiki/howto/monitor/snmp/snmp

[8]http://www.zabbix.com/documentation/1.8/manual/advanced_snmp

[9]http://en.wikipedia.org/wiki/Management_information_base

[10] Rituparna Chaki, "Intrusion Detection: Adhoc Networks to Ambient Intelligent Framework", IEEE 2010

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[11] Jin Shao, Qianxiang Wang, "A Performance Guarantee Approach for Cloud Applications Based on Monitoring"
[12] http://www.monitortools.com/snmp/
[13] http://www.paessler.com/ snmp_monitor
[14]http://www.zabbix.com/documentation/1.8/manual/auto-discovery
[15]http://www.zabbix.com/documentation/2.0/manual/discovery/auto_registration
[16] http://www.net-snmp.org/wiki/index.php/TUT:mib2c_General_Overview
[17] http://www.net-snmp.org/wiki/index.php/TUT:Writing_a_Subagent