International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Smart Alert Monitoring System for Servers and Infrastructure

Sejal Raichura[1], Prof. L. K. Gautam[2], Prof. G. D. Govindwar[3]
[1]PG Scholar, [2]Professor, [3]Assistant Professor, Department of Information Technology, SIPNA College of Engineering, Amravati

Abstract: ***The term infrastructure in an information technology (IT) context refers to an enterprise's entire collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services. Monitoring tools are introduced to monitor these Servers and other hosted services for 24*7 hours. This monitoring tool monitors the servers and the infrastructures which are mission critical for an organization and generates alerts in case of any event occurrence and triggers those events via different medium like – via email, via ticket or notification system. This project introduces a smart alert severity detection system, where our tool would be an add-on feature (or extension/plug-in) to be installed over monitoring tool to monitor and decide the severity of the alert triggered by monitoring tool and which will categorize alerts as per user input for every specific alert as per the requirement. User will have capability to customize the severity and the threshold parameters for the alert.***
Index Terms- Severity, Detection, Infrastructure, Monitoring, Server

I. INTRODUCTION

In today's world, looking into modern business standards in an IT industry, this has been observed that there is a need of developing a framework which will be capable of interacting with the Monitoring tool output and the in-house or external ticketing tool that the infrastructure monitoring team uses to monitor the resources.

The infrastructure nowadays is so widely spread with the complex structure. Infrastructure setup includes servers such as – Web Servers, Database Servers, Domain Controllers and other application hosted servers or app services hosted over the cloud, which are required to be monitored 24*7 hours. As most of these infrastructures are mission critical should be protected from external host attacks and need to be monitored for any service fault or failure because it could make huge business losses if something went wrong even for a small time.

Monitoring tools are introduced to monitor these Servers and other hosted services. This monitoring tool monitors the servers and the infrastructures which are mission critical for an organization and generates alerts in case of any event occurrence and triggers those events via different medium like – via email, via ticket or notification system. Once this alert is triggered to an administrator, administrator starts the initial troubleshooting steps. But the alert could be a fake or false alert, which might increase the administrative task to investigate the issue unnecessarily, where it is not required to be done. So our agenda is to reduce the administrative task and provide meaningful alerts only by discarding the fake or false alerts.

This project introduces a smart alert severity detection system, where our tool would be an add-on feature (extension/plug-in) to be installed over monitoring tool to monitor and decide the severity of the alert triggered by monitoring tool and which will categorize alerts as per the requirement. We will have a framework which will provide us the dashboard to manage the threshold value for the various parameters. This project will be helpful administering the required resources in fruitful way and also will be used to nullify the false alerts.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

Project division in different phases:

A. Study of monitoring tool and infrastructure related components.
B. Database script / query development - To fetch required data from database and associated severity.
C. JAVA programming - To develop logical analysis for triggering notification to appropriate concerned person (Support agent / Administrator) as per severity and information gain from database.
D. To trigger mail alert or web based notification, also to provide input for the database where information is missing in database.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

III. WORKING OF THE SYSTEM

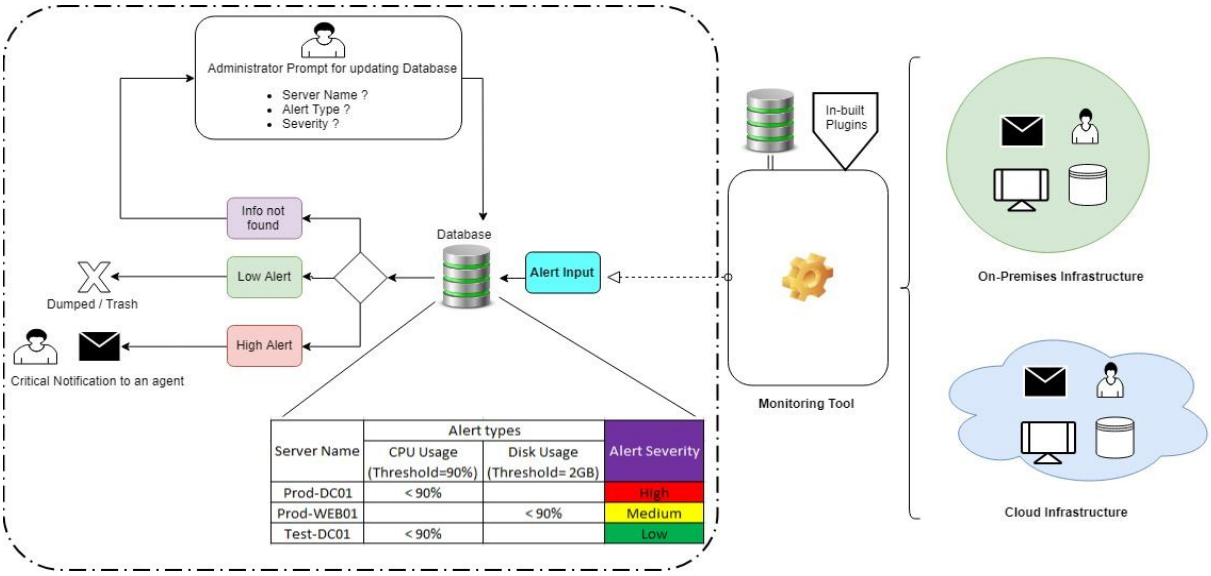


Fig1. Architectural Overview of the system

Activity of the System

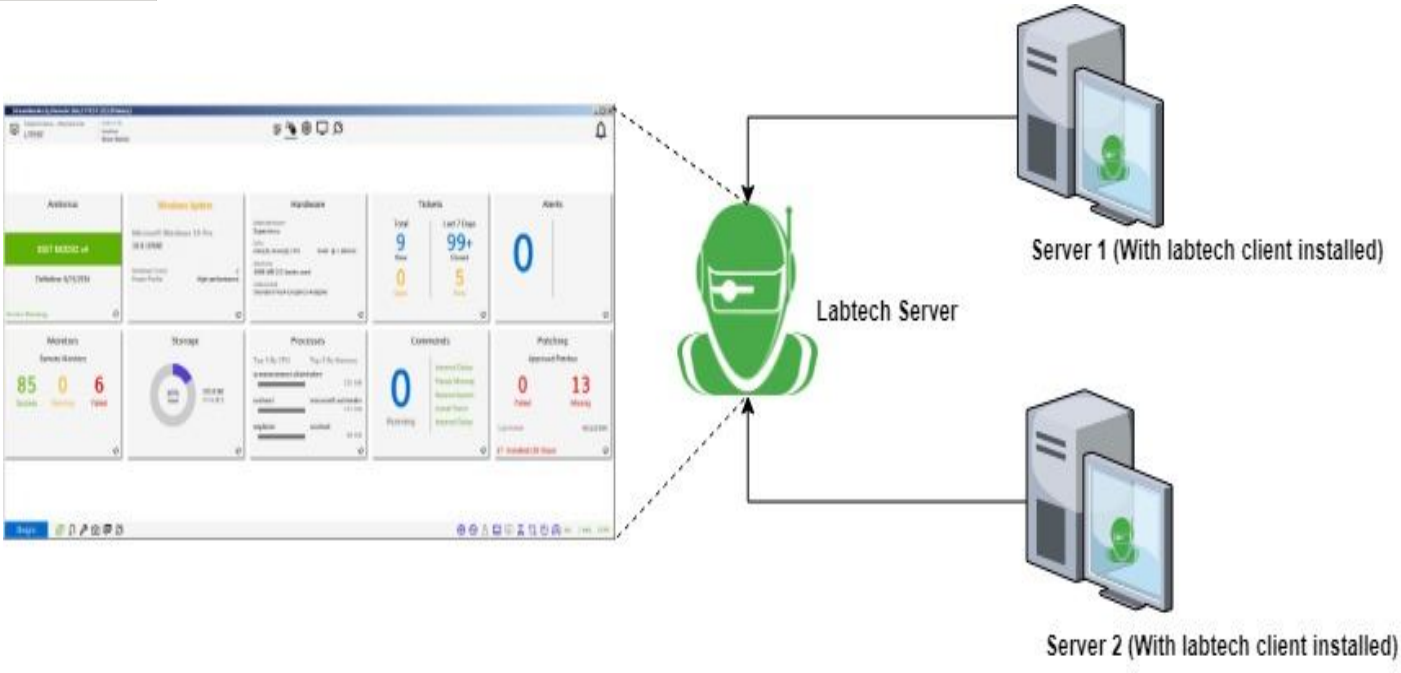
1) Licensing of monitoring tool
2) Login using secured credential
3) Alert input from monitoring tool
4) Data query for the detected alert
5) Type of error:
a) Success – Dump
b) Medium – Query the severity and notify after specific time interval
c) Critical – Query the severity and immediate notification for alert
6) Entry in database:
a) If alert triggered, query database and detect severity, also create log
b) If error not found in database then provide option to troubleshoot
7) Alert severity detection by generating queries to database
8) Sending mail to administration
9) Resending mail to the customer

IV. IMPLEMENTATION

Below are the different aspects which are used in this project implementation and the relatively studied various components to fulfill the requirements of the project:

A. Monitoring Tools

The most important component that we are looking to enhance is the monitoring tool. Exploring different types of monitoring tools for the infrastructure resources were the key role for this project. Different monitoring tools and its functionality was studied from the reference Guides (documentation) provided by each vendors was thoroughly verified. To test the implementation a monitoring tool named as 'LABTECH' is selected here in this project. It is a granular monitoring system for infrastructure components over the cloud or on-premises. One machine (server) will be hosted with the software of this tool. This tool will provide a client application which we need to install on the servers that we want to monitor. The client application will establish commination between server and the respective machine as well as it will monitor the event logs and performance of the end device and share it with the server. If there is any issue or any incident found on the end device this LABTECT server will generate an alert. Alert which will be generated here will be a raw alert where we may not know the severity of the alert as per our monitoring norms that we have planned for our infrastructure components, but here comes the introduction of our framework that we are going to introduce.



B. Framework Language

To create the framework the first thing comes in mind is to decide the architecture and the best preferable language. The feature that we want to develop should be capable of providing visual interface (web based interface) as well as it should be capable of interacting with the database to store and retrieve the information. In our case we are using JSP (Java) to build framework and user interface to update values.

C. Database

The alerts that are generated by Monitoring tool are stored in the database which is there on same LABTECH server, we will synchronize this database records and add one more database and few tables which will be used to build logic for the severity detection. This database will be in sync with our framework to input the user defined threshold if any and to retrieve the information form this database table.

D. Alert Triggering System:

We have used an alert triggering system to send alert to the administrator via different medium – Email, Message, or call. We can even integrate this system with in-house ticketing tool also, if needed.

E. Future Scope of Development

In future we can extend the feature for this project:

1) Showing dashboard on the same portal using analytical tool.
2) Integrating it with ticketing tools.
3) Advanced optimization of generating report for various parameters.
4) Log management.
5) Provide troubleshooting steps by searching it in the reference documents that we have provided.

V. RESULT

Result includes all those activity that take place to convert from the old system to the new. The old system consists of some different operations, which is operated in a very different manner from the proposed new system. A proper implementation is essential to provide a reliable system to meet the requirement of the organization. The implementation plan includes a description of all the activities that must occur to implement new system to put it into operation. It identifies the personal responsible for the activities and prepares a time chart for implementing the system.

OLD SYSTEM	NEW SYSTEM
Currently, traditional monitoring tools in the market may not include integration feature for our in-house tool such as Ticketing tool, analytics and others.	Here, this solution provides us the feasibility to integrate monitoring tool feature and functionality with our in-house tools.
Troubleshooting steps are not provided in the provided results with the alerts.	Alert generated here will also include the troubleshooting steps (which will be the output generate by Google search engine).
Time that an IT engineer requires to find the troubleshooting steps by referring documents or by Google search was greater.	Now, we can save the time of IT engineers by providing the search result from Google for that particular issue and also we can make the system advanced to refer search criteria from our internal reference documents.

TableV.1. Analysis of old System and new System

A. Graphical Representation of Previous System verses Smart System

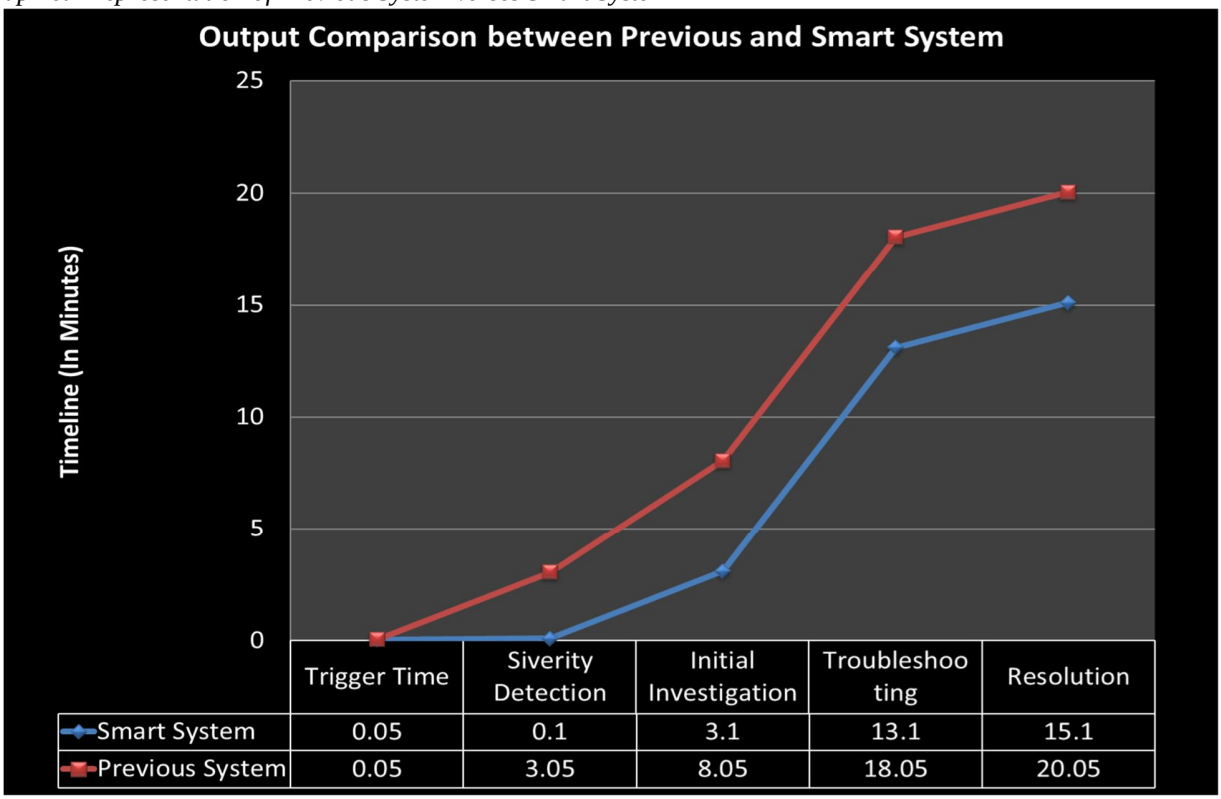


Fig6.1. Comparison between Previous and Smart System

VI. CONCLUSION

This project introduces a smart alert severity detection system, where our tool would be an add-on feature (extension/plug-in) to be installed over monitoring tool to monitor and decide the severity of the alert triggered by monitoring tool and which will categorize alerts as per the requirement. We will have a framework which will provide us the dashboard to manage the threshold value for the various parameters. This project will be helpful administering the required resources in fruitful way and also will be used to nullify the false alerts. and administration work for IT team is reduced and organization can utilize IT team for other tasks, this will increase the efficiency of IT and ultimately benefit organization

VII. ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind of support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them. I am highly indebted to Prof. L. K. Gautam for their guidance and constant supervision as well as for providing necessary information regarding the project and also support in completing the project and co-guide Prof. G.D. Govindwar, who provided me constructive and positive feedback during the preparation of this project. I would like to express my sincere thank to Dr. V. S. Gulhane, Head of Department (Information Technology) and all other staff member of Information Technology Department for their kind co-operation. I would like to thank to The Principal of our institution for providing necessary facility during the period of working on this project. Last but not least, I am thankful to my friend and Library staff members whose encouragement and suggestion helped me to complete my project. I am also thankful to my parents Mr. Chandresh C. Raichura and Mrs. Smita Chandresh Raichura whose best wishes are always with me. I am also thankful to my husband Mr. Gaurav H. Kariya and my in-laws who motivate me to complete my project.

REFERENCES

[1] Shicong Meng, Ling Liu, "Enhanced Monitoring-as-a-Service for Effective Cloud Management", Proc. IEEE Computer Society,pp. 1705 – 1720, 2013.
[2] Shicong Meng, Srinivas Raghav Kashyap, Chitra Venkatramani,"Resource-Aware Application State Monitoring", Proc. ,pp. 2315 – 2329, 2012.
[3] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: Clustering analysisof network traffic for protocol- and structure-independent botnet detection," in USENIX Security Symposium, 2008, pp. 139–154.
[4] G. Ren, E. Tune, T. Moseley, Y. Shi, S. Rus, and R. Hundt, "Google-wide profiling: A continuous profiling infrastructure for data centers," IEEE Micro, vol. 30, no. 4, pp. 65–79, 2010.
[5] N. Jain, P. Mahajan, D. Kit, P. Yalagandula, M. Dahlin, and Y. Zhang, "Network imprecision: A new consistency metric for scalable monitoring," in OSDI, 2008, pp. 87–102.
[6] Amazon CloudWatch, "https://aws.amazon.com/cloudwatch/features/".
[7] C. Estan and G. Varghese, "New directions in traffic measurement and accounting," in SIGCOMM, 2002, pp. 323–336.
[8] Microsoft Azure Monitor "https://docs.microsoft.com/en-us/azure/azure-monitor/".
[9] N. Jain, L. Amini, H. Andrade, R. King, Y. Park, P. Selo, and C. Venkatramani, "Design, Implementation, and Evaluation of the Linear Road Bnchmark on the Stream Processing Core," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), 2006.
[10] B. Hayes, "Cloud Computing," Comm. ACM, vol. 51, no. 7, pp. 9- 11, 2008. L. Amini, N. Jain, A. Sehgal, J. Silber, and O. Verscheure, "Adaptive Control of Extreme-Scale Stream Processing Systems," Proc. IEEE 26th Int'l Conf. Distributed Computing Systems (ICDCS), 2006.