ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 4, April 2016**

# Evaluation of Integrated Monitoring System for Application Service Managers

Prerana S. Mohod, K. P. Wagh, Dr. P. N. Chatur

M.Tech Student, Dept. of Computer Science and Engineering, GCOEA, Amravati, Maharashtra, India

Assistant Professor, Dept. of Information Technology, GCOEA, Amravati, Maharashtra, India

Associate Professor, Dept. of Computer Science and Engineering, GCOEA, Amravati, Maharashtra, India

**ABSTRACT:** In recent search, physical/ virtual devices are affected to each other and share with data centre. Therefore historical data saving is very important for that integrated monitoring system. Existing system uses different monitoring software for processing of historical data. So it requires more transition time for switching from one historical data to using different monitoring software. The Integrated monitoring software is used for processing and collecting of data on historical data. In this system historical data arrange in five basic formats and that format help the application server managers to manage 98.16% of monitoring tasks. This result suggests that the integrated monitoring software is used effectively for reducing transition time, the cost of monitoring software and enhancing service availability of systems.

**KEYWORDS**: Integrated Monitoring System; Monitoring Tasks; Basic data format.

## I. INTRODUCTION

In today's data centers, with the emergence of recent virtualization technologies [7], existing systems are being integrated into a small number of large data centers. A small number of hardware devices are provided to users through private networks or the Internet in such huge data centres, a huge number of applications. This type of facility is called as Software as a Service (SaaS) Platform. It becomes more important than ever before to monitor applications on virtual devices given in this paper, a system that provides this type of service is referred [2].

In SaaS Model, if performance of application affected by physical or virtual resources then it directly affects on other applications which sharing same resources. Therefore, to avoid system failure due to mutual application and resource dependency, application service managers of system have to spend lot of time monitoring the applications related to physical or virtual resources.

In conventional monitoring system regular time series data and event log data are monitored by different monitoring software. Therefore application service managers have to spent time for moving from one monitoring tool to another for collecting and processing data. Regular time series data contains CPU usage, Disk usage, number of active sessions on web servers and they are periodically measured. While event log data contains alerts, starts and ends of batch processing, access of web applications, logins to web portals. Combination of regular time series data and event log data are called as Historical data.

The target of this study states that Integrated monitoring software is designed for collecting and processing of historical data to shorten the transition time (the time to switch from one historical data to another) with five basic data formats.

## II. RELATED WORK

In [1] states historical data are combination of Regular time series data and Event log data. However, in existing system Regular time series data are performed by SNMP protocol and Event log data are performed by Syslog. Therefore existing system required more time for switching from one historical data to another. Therefore, integrated monitoring software is proposed to shorten transition time.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Integrated Monitoring System is a monitoring service for applications and resources. It supports custom related applications, which include numerical data, statistical values, and string key-value pairs called dimensions. These application related services have high flexibility for representing structured historical data. They are useful for implementing the integrated monitoring software. In these system use sales and purchase module data set. It gives users related data with respect to their transaction of purchase items. This Platform is used for design of integrated system. Here it classifies log level monitoring like error log, system log etc. The classification of log is based on type of historical data. It includes all logs which affect on system performance. It gives access logs of users, authenticate user's logs, number of active users log, access count of web application, transaction logs and root cause of failure logs. The extraction of log is based on some data mining techniques (i.e. Naïve Bayes classification algorithm.)

## III. PROPOSED INTEGRATED MONITORING SYSTEM

### A. *Monitoring Tasks*

The application service managers perform various different kinds of tasks called monitoring tasks. There are majorly five different types of monitoring tasks such as Failure detection, Anomaly detection, Root cause analysis, Performance prediction and Impact analysis. These five major monitoring tasks have been defined [1]. Figure 1 shows working of the monitoring tasks.

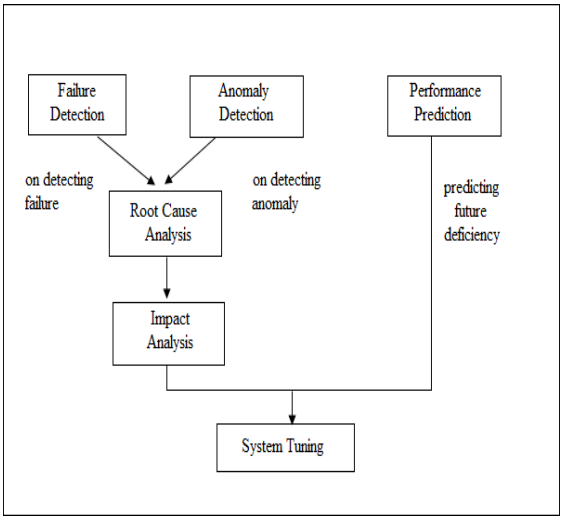


Figure 1.Working of Monitoring Tasks.

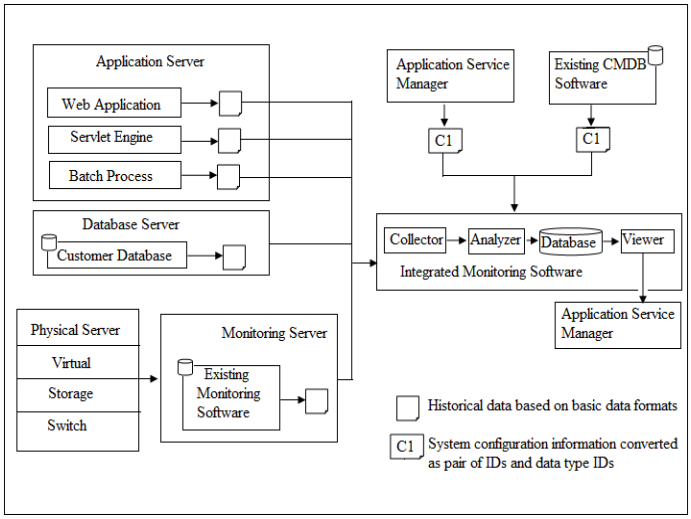


Figure 2. System Architecture for Integrated Monitoring Software.

Failures cause serious problems on system's service like service shutdown or degradation of quality of service. Failures are checked manually by operators or received an alert from monitoring software. If a failure is detected, they inform infrastructure or service managers about the failure. If any application server or database server is not running (i.e. unplanned downtime).Then it is critical problem. It directly affects service quality. Then in these case alert generated by monitoring software so as to take correct action with respect to failure immediately.

Anomaly does not cause serious problems. Anomaly has been defined as variation from the normal or usual order. The normal behaviour of system performance indicator values is less than threshold value. If performance indicator values reach to threshold and exceeded from normal value, then anomaly is detected. Here it checks any unauthenticated users tried to access transaction activity. If any unauthenticated user is detected, then system will be blocked that user [8].

The system performance degradation and then plan to compare and change system configuration or buy additional hardware with expected growth of load in near future, the application service managers predict performance deficiency. For example if CPU utilization is 95% in today's date. Then after some time or tomorrow there is capability that it may be goes up to 100 %. Due to these downtime of system will occur. The Solution to resolved performance problem is increase the additional ram or use additional processor. The Monitoring software predicts the performance of system with the performance indicator's threshold value; check the increasing tendency of system load in recent month and with the overall system log analysis. It also predicts system performance as considering response time as parameter. It checks delay in response time with respect to transaction performed by user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 4, April 2016**

Application service managers analyse actual the cause of occurrence of anomaly or failure. In order to study main cause, most of times, managers have to search minute details such as old logs analysis and process level statistics of historical data It also involves run-time analysis, code profiling and need real-time process level statistics to monitor. If any transaction activity is failed, then system will check cause of failures like long running transaction, unauthenticated user, incorrect security pin, and system downtime.

From the point of view of hardware, software and customers data, application service managers analyse the impact of occurrence of failure or anomaly on system. For example, if any transaction is fail, then the managers have to find services and customers affected by the failure.

B. *System Architecture*

System architecture of monitoring software for application service managers is shown in Figure 2. Integrated monitoring software consists of collector, analyzer, database and viewer. Collection of historical with five basic data formats are done by collector. Creation of well-organized historical data and relation data are performed by analyzer. Then these data are inserted them into database. These data are then displayed to application service manager by viewer. Servlet Engine outputs historical data about application and middleware according to basic data formats. Database server converts customer data into basic data formats. Monitoring server converts existing physical or virtual services of data into basic data formats. All these data about applications and physical or virtual services are converted into basic data formats and collected into integrated monitoring software. Application service managers converted configuration information documents into pairs of IDs. Management server converted existing configuration information into the pairs of IDs with existing management software such as CMDB (i.e., Configuration Management Database software).

C. *Operations Performing on Historical Data*

There are two types of operations performing on historical data and they are collection and processing of historical data.

In collection of historical data includes examples of historical data i.e. CPU usage, memory usage, network bandwidth usage, disk usage, Performance data such as number of active connections to database, available memory and number of active sessions, Start time, execution time, number of processed data and user uploaded data of each batch process, access count and execution time of each web page or function, detailed logs and login histories of each web application.

Processing of historical data further divided into two types and they are well-organized historical data and relation data for historical data. Well-organized historical data managed historical data into proper format like line charts, indexes for filtering and sorting logs, and statistical values from regular time-series data and event log data for these developing new programs. In the processing of relation data also customize an alignment sequence of historical data with monitoring software to easily associate the relations between the data. For example, relations between services and physical/ virtual servers, relations between load balancers and web servers, relations between web servers and database servers and connections between network ports of physical/virtual devices are needed.

D. *Basic Data Format*

The Basic data format is essential for properly investigating monitoring tasks. In existing system only two basic data formats are used and they are performance data and response data. So it takes lot of time for monitoring tasks. Whereas, integrated monitoring system supports five basic data formats. Five basic data formats are performance data, response data, command execution data, web event log data and login histories data. The performance data is a data type for representing a simple performance value. The data collected by monitoring software are converted into performance data. The command execution data is a data type for representing the detailed result of batch processing. The web event log is a data type for representing customers' operations of web applications and execution times evaluated at the web servers. It can include a number of descriptions about the customer's operations. The login history is a data type for representing the login time and the logout time of each customer. The response data is a data type for representing response times.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

## IV. RESULTS AND SURVEY

The survey held by application service mangers evaluated performance result [6]. In these surveys, application service manager asked questions about how frequently monitoring occurs, how to detect failure or anomaly in system, what actions to be taken when any anomaly or failure occurs and so on. After that application service managers estimate transition time required for monitoring tasks of historical data and evaluate results. Existing system supports only performance data and response data. Therefore it covers only 69.6% of monitoring tasks of basic data format of historical data. Integrated monitoring system supports all five basic data formats. Therefore it almost covers 98.16% of monitoring tasks of basic data format of historical data.

TABLE I. DATA SAMPLE LOGS OF TRANSCATION

| Data Sample log | Frequency count | Transition time(in millisecond) | Total transition time for transaction log(T) |
|---|---|---|---|
| Performance data (A) | 3 | 210545 | 1513485 |
| Response data (B) | 11 | 788861 | 1513485 |
| Command execution data(C) | 2 | 218845 | 1202133 |
| Web event log(D) | 7 | 290024 | 1513485 |
| Login histories data(E) | 3 | 5210 | 1513485 |

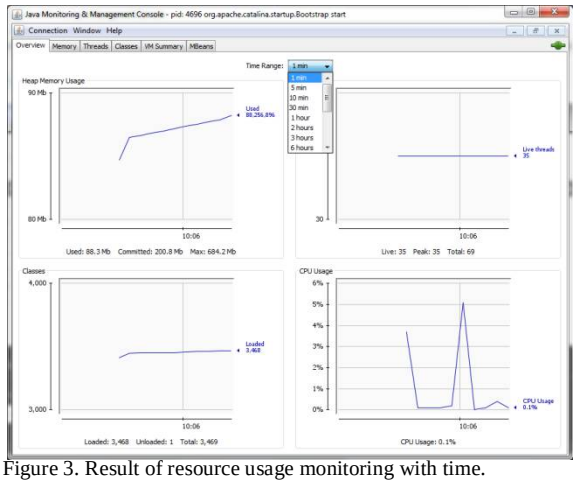

Figure 3. Result of resource usage monitoring with time.

TABLE I shows sample logs of transaction process by users. It gives frequency count ,transition time and total transition time of performance data(A),response data(B),command execution data(C),web event log data(D) and login histories data(E) respectively by using queries fetched by user from database. Figure 3 shows number of CPU usage, classes loaded, heap memory usage, thread usage with specified time.

TABLE II. PERFORMANCE PREDICTION EVALUATION

| Basic data format | Transition time (Tn) | Transition time Tn=Tn-T(where T=210545 ) | Performance prediction ((T1-Tn)) /T1*100 |
|---|---|---|---|
| A&B | 210545 | T1=1513485(first) | 86.08 |
| A&B&C | 429390 | T2=167030 | 85.54 |
| A&B&D | 500563 | T3=290018 | 80.83 |
| A&B&E | 215755 | T4=5210 | 99.65 |
| A&B&C&D | 719414 | T5=508869 | 66.37 |
| A&B&C&D&E | 5210 | T6=5210(Last) | 99.65 |

TABLE II calculated performance prediction of basic data format by using transition time. In first transition of basic data format completeness rate of performance prediction of A&B calculated by using $((T1 - T)/T1) * 100$ and other transition of basic data format calculated by using $((T1 - Tn)/T1) * 100$.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

TABLE III. MONITORING TASK COMPLETED IN INTEGRATED SYSTEM

| Basic data format | Monitoring Tasks | | | | | |
|---|---|---|---|---|---|---|
| | Anomaly Detection | Performance Prediction | Root Cause Analysis | Impact Analysis | Other | All Types |
| A&B | 100 | 86.08 | 44.11 | 100 | 55.88 | 77.21 |
| A&B&C | 100 | 85.54 | 52.94 | 100 | 47.05 | 77.10 |
| A&B&D | 100 | 80.83 | 64.70 | 100 | 35.29 | 76.16 |
| A&B&E | 100 | 99.65 | 70.58 | 100 | 29.41 | 79.93 |
| A&B&C&D | 100 | 66.37 | 73.52 | 100 | 73.52 | 82.68 |
| A&B&C&D&E | 100 | 99.65 | 100 | 100 | 91.17 | 98.16 |

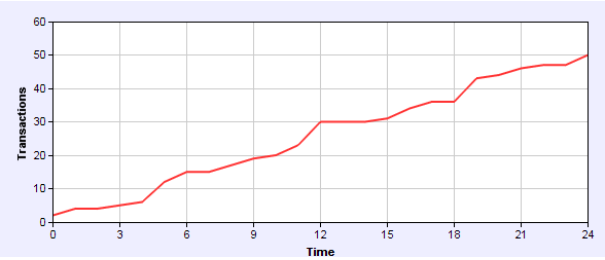

Figure 4.Time required for transactions of Integrated Monitoring software.

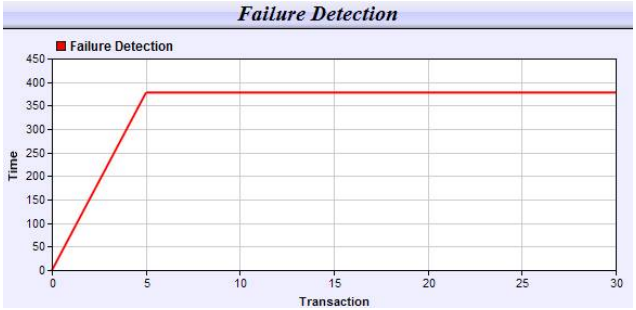

Figure 5.Results of Failure Detection in Integrated Monitoring Software.

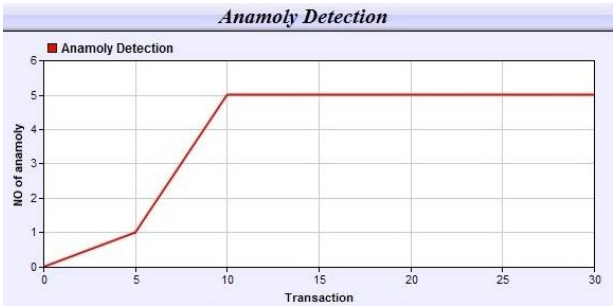

Figure 6.Results of Anomaly Detection in Integrated Monitoring Software.

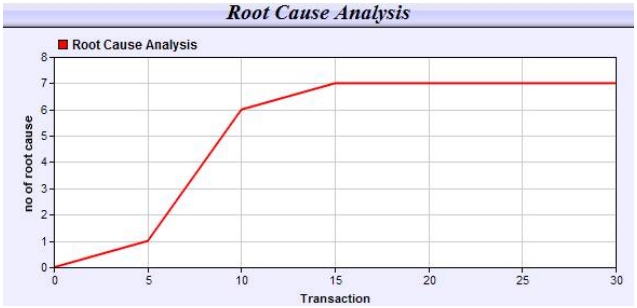

Figure 7.Results of Root Cause Analysis in Integrated Monitoring Software.

TABLE III calculated completeness rate of all types of monitoring task with basic data format. Root cause analysis is percentage ratio of frequency count of basic data format to total frequency count of transaction log occurred. For example Root cause analysis of A and B is calculated using total frequency count of A and B to the total frequency count of transactional log. Anomaly detection is calculated using total number of anomaly detected in system accurately or not. For example unauthenticated user tried to access system, then system blocked that user for transaction. Anomaly is calculated using number of failure of transaction with respect to that user with specific time. Impact analysis is estimated based on all the transaction activity is detected by system accurately. If any transaction in system affects system continuity then system takes further action so as they didn't affect on system performance. Other log calculated remaining logs of transaction to the total transaction logs of system.In Figure 4 shows transactions of integrated monitoring software and their required time. The graph shows time respect each transaction in integrated monitoring software. Figure 5 shows how many failures occur in system with respect to each transaction. It shows results of failure detection in system with respect to time. Figure 6 shows anomaly detection in system. It shows number of anomaly occurs with respect to transaction. Figure 7 shows actual cause of anomaly or failure detection in system so as to resolve anomaly or failure.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 4, April 2016**

## V. CONCLUSION

Integrated monitoring software evaluated historical data was proposed for shortening operation times. Well-organized historical data before the application service managers' requests could shorten the transition times which surveys on current monitoring tasks for over many companies showed; creating relation data for recommendations could shorten the transition times; and a grouping of the two types of processing had a stronger effect on the transition times than either of them individually. In monitoring software for application service managers recommended to implement both types of processing. The results of survey show that proposed integrated monitoring system with all of the basic data formats supports 98.16% of monitoring tasks. The reduction rates of the transition times were higher than the ones in the case of other monitoring tasks contain root cause analysis and impact analysis. The proposed integrated monitoring software results suggest particularly effective in mission-critical application services.

## REFERENCES

1. Masahiro Yoshizawa, Tatsuya Sato and Ken Naono, "Integrated Monitoring Software for Application Service Managers", IEEE Transaction on Network and Service Management, Vol. 11, No. 3, pp. 321-332, September 2014.
2. M. Armbrust, A. Fox, R. Griffith, "Above the clouds: A berkeley view of cloud computing", University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, Feb 2009.[online].Available:http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.
3. Alina Girbea, Constantin Suciu, "Design and Implementation of a Service-Oriented Architecture for the Optimization of Industrial Applications", IEEE Transaction on Industrial Informatics, Vol.10, No.1, pp.185-195, February 2014.
4. Mehdi Mirakhorli, Jane Cleland Huangy, "Detecting, Tracing, and Monitoring Architectural Tactics in Code", IEEE Transaction on Software Engineering, pp. 1-18, 2015.
5. B. Krishnamurthy, A. Neogi, "Data tagging architecture for system monitoring in dynamic environments", In Proc. NOMS, 2, pp. 395–402, 2008.
6. M. Yoshizawa and K. Naono, "Design and evaluation of integrated monitoring software for SaaS-based systems", In Proc. APNOMS, pp. 1–4, 2011.
7. VMware vSphere. [Online]. Available: http://www.vmware.com/products/vsphere/
8. P. Kavita, M. Usha, " Anomaly Based Intrusion Detection in WLAN using Discrimination Algorithm Combined with Naïve Bayesian Classifier" , Jounal of theoritical and applied Information Technology, Vol.61,No. 3, pp. 646- 653, 31 st March 2014.