AN EFFICIENT SECURITY OPTIMIZATION MODEL FOR SERVER STORAGE MONITORING IN MODERN CLOUD COMPUTING

K. Vengatesan, Amit Sampat Nirmal and Raghvendra Naidu
Department of Computer Engineering, Sanjivani College of Engineering, India

Abstract

Cloud server monitoring is essential because it enables accessibility and adaptability to online resources, which are essential parts of business operations. End users may require content controlled by cloud servers. Therefore, cloud server monitoring is a necessary part of ensuring the functionality and productivity of applications and services in line with the company needs for day-to-day business operations. Slow servers can directly affect a company finances, as end users may quickly abandon slow cloud pages. A cloud server monitoring platform like data is designed to detect errors and failures. In this paper, an efficient security optimization model was proposed for server storage monitoring in modern cloud computing. The platform sends alerts or notifications to network administrators to avoid any kind of server downtime. Cloud server monitoring generates insights based on demand and shows changes in traffic to multiple cloud sites, applications, and software. Tracking data such as cloud site activities and sessions can be helpful for companies looking to extend their cloud sites, modernize application functionality, or add additional services to meet the needs of increased traffic.

Keywords:

Cloud, Server, Monitoring, Online, Business, Finances, Errors, Failures

1. INTRODUCTION

Visualize recent and failed backups, device distribution, failure trends and more in one unified platform. Run dashboard reports by exporting dashboard insights to PDF/CSV files. It enables configuration management systems to deploy report, detect out-of-process changes, perform audits and backups [1]. Configure your network with AI-Driven network automation, making your network smarter and healthier than ever. Automated configuration for changeover, backup, and restore Simplify repeated complex configuration changes instead of manually operating multiple devices [2-3]. Python integration makes run book reading advanced and empowering with monitoring and debugging capabilities. Always stay alert with smart alert system. Stay one step ahead and solve problems before any damage is done [4]. Stay up-to-date on configuration changes with alerts and view changes made [5]. Use role-based access to fully control who can make changes to devices and configurations. Configure audit logs and gain powerful actionable insights with audit reports [6]. The tool notifies whenever there is a change in device configuration, thereby helping to quickly replace a failed component. Find a backup file quickly by simplifying processes like highlighting configuration errors, scheduling regular backups, and running archive scripts [7]. Improve overall network security by easily identifying vulnerabilities through vulnerability assessment. Assess and enforce compliance with critical security standards using OOB reports for FISMA, PCI DSS, etc [8]. Pre-integrated support for well-known network device vendors. Maintain full configuration history of devices. Users can compare device configurations to ensure compatibility and standardization [9-10]. Network automation is the practice of automating the process of configuring, managing, testing, maintaining, and operating networked and connected devices.

A good network automation solution aims to scale the IT infrastructure without adding any new IT management staff or devices. The dependency and complexity of the network makes it critical to configure and automate it properly. A good network automation solution can improve the performance and maintain good health of your network. With the number of failures and challenges, it needs an automated system and it helps your business grow. Cloud service providers such as Amazon, Microsoft Azure, and Google help IT companies scale their storage, networking, servers, and virtual hosting capabilities by offering Infrastructure as a Service (IaaS). Tracking operations and transactions is important to avoid failure when it comes to deployment and dependencies. As a large number of servers are deployed in the cloud, security and availability become important concerns. Additionally, the number of endpoints and cloud-deployed applications can be a gateway for attackers, leading to network security breaches. Therefore, it is imperative to monitor network performance and availability, secure the network to improve user experience, and have minimal downtime.

2. RELATED WORKS

The agent less collection enables you to effortlessly collect process and correlate your metrics, log messages and events across network devices, computers, virtualization and the cloud in one central location. Lightning-fast auto-detection and configurations will get you up and running in minutes [1]. It also provides basic functionality to monitor resource usage and critical metrics on predefined & customizable dashboards. By combining machine learning and analytics, you have the power to extract signals from alarm noise [2]. Built-in ML algorithms provide anomaly detection and actionable intelligence. Powered by Infrastructure Monitoring, it keeps your infrastructure healthy, smart, and anything and everything that keeps your business growing. Integrated NMS services provide a highly scalable AI-driven solution for service assurance, orchestration & automation, helping organizations achieve their network management objectives [4]. it gives you network monitoring capabilities with a comprehensive application and infrastructure overview, so you can identify and fix problems quickly.

Infrastructure monitoring is a process that involves collecting and analyzing data from various sources to detect potential issues such as performance issues or security breaches [5]. As a result, monitoring the system infrastructure ensures system availability, good health and minimal downtime. Quality of Service (QoS) defines the growth of any organization and depends on how well the infrastructure is managed and monitored [7]. Various

components such as connected devices, networks, applications, servers, storage, operating system etc. form a comprehensive ecosystem to monitor infrastructure. Monitoring the infrastructure makes it easy to identify the root cause of any failure and resolve it before users experience any downtime [8]. Despite measuring time and cost-effectiveness, the infrastructure monitoring solution depends on various criteria that the monitoring solution should have [11]. A good monitoring solution can monitor the heart and soul of the operation and address potential failures. The solution helps reduce costs by monitoring infrastructure, reducing downtime and improving uptime. Less vulnerability protect infrastructure and improve customer satisfaction. In addition, the monitoring process helps improve productivity by improving response time and resolving more fatal errors [10].

3. PROPOSED MODEL

The main purpose of cloud server monitoring is to protect servers from potential threats and failures. A cloud server monitoring platform helps organizations by collecting performance metrics from every server included in the IT infrastructure, which can be used to monitor the overall performance and health of the devices. There are two types of metrics cloud server monitoring sites monitor. This was shown in the Fig.1.

- Connection Metrics: Monitors connections such as request rate, response time, response size, and active connections between the server and users.
- Host Metrics: Measure the health of devices, applications and/or cloud sites hosted on cloud servers, including uptime, CPU usage, memory usage, cache and threads.

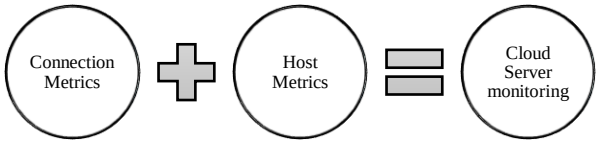

Fig.1. Metrics of metrics cloud server monitoring

Cloud server monitoring measures user load, overall performance speed, and the security level of servers. It gives companies the insight to detect and fix issues and potential threats before they affect the end-user experience. A cloud server monitoring platform includes a wide range of features that automatically provide critical and actionable insights from the performance of all cloud servers in an IT infrastructure. Such a cloud server monitoring practice matches historical logs with real-time data, allowing network administrators to quickly identify unusual events or behavior and which part of the server is experiencing downtime. It provides insightful details on all important server performance parameters such as hard disk capacity, CPU usage, memory usage and bandwidth usage from an intuitive cloud console. It provides comprehensive data collection capabilities in both agent and agent less modes across cloud and hybrid infrastructure. This was shown in the Fig.2

- Access monitoring applications for thousands of devices and technologies across your network, server, application and cloud layers.
- Collect everything with agent or agent less collection including metrics, logs, events, and traffic and streaming data.
- Eliminate point tracking tools by bringing all your tracking data in one place to gain deeper visibility.

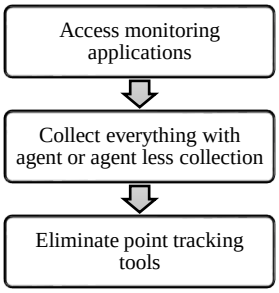

Fig.2. Data collection capabilities

The server performance monitoring allows a system admin to stay on top of server downtime and performance issues. This server monitoring platform has the ability to monitor all types of IT infrastructure servers in both consolidated and distributed workload scenarios. Identify server performance issues such as resource usage, application downtime, and its average. It provides an alert facility to keep IT support staff and all stakeholders up-to-date and notify them of potential threats, resource shortages and other service issues. IT teams need the right event environment to confidently identify critical and not-so-critical issues. This was shown in the Fig.3.

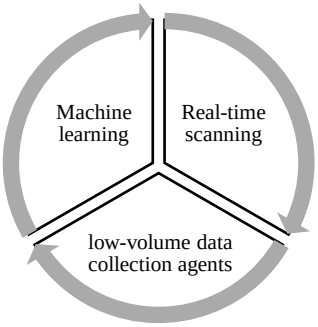

Fig.3. Confidently identify the issues

- Machine learning-powered alerting provides capabilities to extract meaningful insights to separate signals from noise.
- Real-time scanning automated discovery and dependency mapping to correlate IT service dependencies.
- On low-volume data collection agents – sub-second for rapid identification and resolution.

It provides dashboards and reports that allow organizations to instantly view performance metrics for analyzing cloud servers. It helps deliver better business outcomes through data-driven insights, with a single and common platform for monitoring, log indexing, visualization and alerting of all events across hybrid infra. It allows you to discover and monitor cloud services, VMs, containers, networks, devices, logs, events and more under one advanced AI-powered platform. With auto-discovery and pre-defined monitoring applications, your hybrid infra resources can be seamlessly integrated into real-time.

- Topological views: See constantly changing IT relationships based on discovery protocols and network traffic interactions.
- Dashboards & Reports: Comprehensive visualization and dashboard capabilities take your monitoring experience to the next level with no query language required.
- Advanced Data Explorers: Advanced and AI-driven data explorers help you understand data and track the impact of every metric/process running in your stack.

Such reasons make it imperative to monitor servers installed on premises or in the cloud. Monitoring servers helps organizations protect servers. Based on the type of server, various metrics can be monitored and measured, helping organizations protect servers from potential damage.

4. RESULTS AND DISCUSSION

The proposed security optimization model (SOM) was compared with the existing Improved Firefly Algorithm (IFA), cyber-physical systems with cloud support (CPSCS), Cost benefit analysis of cloud computing (CBACC) and control and communication management (CCM)

Memory Usage Management: Due to the large number of transactions and blocks being used every second, it is important to ensure that the system has sufficient CPU power and memory. Excessive consumption of memory can affect user experience and performance. Agent-based monitoring requires an agent to be assigned to each server. This was shown in the Table.1,

Table.1. Comparison of Memory Usage Management

Inputs	IFA	CPSCS	CBACC	CCM	SOM
100	54.10	49.43	91.07	63.01	90.00
200	52.61	47.46	88.65	60.81	88.01
300	51.81	46.33	88.24	60.01	86.81
400	49.51	45.20	86.64	59.34	86.33
500	48.47	44.75	84.32	57.91	84.90
600	47.83	43.30	83.07	56.82	84.74
700	47.17	42.82	80.34	56.34	82.97

Agent based monitoring is more secure as compared to agent less monitoring. The agent handles all security aspects and controls all communications. Since it is built into the application/operating system, no external firewall rules need to be applied. Agent-based monitoring comes with broader and deeper monitoring solutions.

Server Failure management: If the servers fail to perform the requested actions, it may lead to failure of some critical functions. For example, if the server cannot collect the product details from the database, users cannot view the product details, which destroy the user experience. Based on the cloud server and the monitoring tool, the server monitoring technique differs. As an organization grows and the number of deployments and volumes increases, it needs to set up a server monitoring solution that collects data from various cloud-based endpoints. This was shown in the Table.2.

Table.2. Comparison of Server Failure management

Inputs	IFA	CPSCS	CBACC	CCM	SOM
100	43.30	54.89	71.55	59.48	91.13
200	43.41	55.39	71.55	60.57	91.39
300	43.47	56.14	72.38	61.71	91.96
400	43.52	56.14	71.65	61.35	90.82
500	43.56	55.09	70.54	59.82	89.80
600	43.59	54.81	70.14	59.18	89.56
700	43.61	55.53	70.71	59.76	90.21

Now that the board of directors has been notified of the failure, it is time to take action against it. A monitoring solution can analyze the root cause from available data and help resolve issues. Before that, a policy needs to be configured. A policy that lays down a procedure for responding to alerts. Explore security alerts, solutions for operational failures, alert types, response actions, and priority. These can be part of the policy when configuring the go-to action procedure.

Accessibility Management: Adequate bandwidth and server availability is essential. By pinging the server, the server reach ability and its response time can be measured. Agent less monitoring requires only the use of software on the remote data collector. The data collector communicates with target systems on various ports. Collector may need to be installed with administrator access to access remote systems. Agent less monitoring comes with its own limitations as not all applications and operating systems support it. This was shown in the Table.3,

Table.3. Comparison of Accessibility Management

Inputs	IFA	CPSCS	CBACC	CCM	SOM
100	46.77	62.59	69.61	56.67	84.87
200	49.19	64.79	71.60	58.16	86.84
300	49.60	65.59	72.80	58.96	87.97
400	51.20	66.26	73.28	61.29	89.18
500	53.52	67.69	74.71	62.30	89.55
600	54.77	68.78	74.87	62.94	91.08
700	57.50	69.26	75.64	63.60	91.58

Response Time management: Getting a quick response from a server is important, especially when there are many transactions and dependencies happening at a given time. Before, any monitoring solution can start monitoring a computer and estimating metrics, it needs basic configurations to be set up. One of the initial steps in configuring the system is to divide agent-based devices into two: agent-based devices and agent less devices. This was shown in the Table.4.

Table.4. Comparison of Response Time management

Inputs	IFA	CPSCS	CBACC	CCM	SOM
100	38.59	66.06	86.58	53.21	86.84
200	38.70	66.04	86.75	53.48	87.34
300	38.72	65.16	86.02	53.18	87.22
400	35.62	62.33	82.68	49.67	83.99

500	34.42	61.01	81.95	48.35	83.61
600	33.81	60.18	81.06	47.81	83.04
700	33.40	59.78	80.98	47.51	83.34

It is important to identify the metrics to be monitored. One should prioritize metrics that help monitor servers and provide important insights into server behavior. The choice of metrics depends on the type of infrastructure and services the company uses. For example, an application server will need metrics like server availability and response time, while a monitoring tool for a cloud server will measure capacity and speed.

Security management: A successful or failed authentication can provide insights into the system performance. Both efforts help administrators better protect the system. Once metrics are prioritized and tracked, the next step is to set threshold values for them. A base value and a certain range should be set according to the type of measurement. This was shown in the Table.5.

Table.5. Comparison of Security management

Inputs	IFA	CPSCS	CBACC	CCM	SOM
100	37.21	66.53	84.23	50.02	91.00
200	35.58	64.79	82.65	48.60	89.71
300	35.10	62.45	80.45	47.34	88.70
400	33.81	61.64	78.82	45.35	87.81
500	31.70	59.35	77.68	42.88	87.44
600	30.21	57.42	75.48	41.44	85.80
700	28.40	55.69	74.33	39.72	85.43

Based on these baseline values, upcoming server performance can be monitored. As the server is monitored and metrics are measured, the next step is to set an alert when a certain threshold is met. An alert system that sends notifications to the admin team when any metrics reach a threshold value or any security breach occurs.

5. CONCLUSION

A server monitoring tool should be configured to seamlessly collect data from cloud endpoints. A server monitoring tool monitors server-wide activity with the help of log files. Log files contain data about failed operations and user actions. Also, metrics like network connectivity and CPU performance can be monitored with the help of log files. Additionally, log files help protect the server as they contain information about security events. With these procedures, IT organizations can monitor the server, ensure smooth transactions across the server, improve user experience and protect the server from data breaches. Being such an intelligent monitoring tool, it provides monitoring solutions with cutting-edge technologies like artificial intelligence and machine learning. Anticipates potential errors, checks server health, informs management team, and helps resolve them before they cause any potential damage. The combination of AI and ML makes it a smart monitoring tool that provides an integrated dashboard with smart widgets and real-time data from measured metrics. Overall, server monitoring is essential when your entire business and transactions depend on the server health.

REFERENCES

[1] K. Alhamazani and V. Bhatnagar, "An Overview of the Commercial Cloud Monitoring Tools: Research Dimensions, Design Issues, and State-of-the-Art", *Computing*, Vol. 97, No. 4, pp. 357-377, 2015.

[2] F. Rabbi and M.A. Bassey, "Gaussian Map to Improve Firefly Algorithm Performance", *Proceedings of Control and System Graduate Research Colloquium*, pp. 88-92, 2022.

[3] Z. Guoli and L. Wanjun, "The Applied Research of Cloud Computing Platform Architecture in the E-Learning Area", *Proceedings of International Conference on Computer and Automation Engineering*, pp. 356-359, 2010.

[4] J. Wan and J. Lloret, "Context-Aware Vehicular Cyber-Physical Systems with Cloud Support: Architecture, Challenges, and Solutions", *IEEE Communications Magazine*, Vol. 52, No. 8, pp. 106-113, 2014.

[5] D.G. Chandra and M.D. Borah, "Cost Benefit Analysis of Cloud Computing in Education", *Proceedings of International Conference on Computing, Communication and Applications*, pp. 1-6, 2012.

[6] M.H. Mohamaddiah, S. Subramaniam and M. Hussin, "A Survey on Resource Allocation and Monitoring in Cloud Computing", *International Journal of Machine Learning and Computing*, Vol. 4, No. 1, pp. 31-38, 2014.

[7] J. Wan and J. Lloret, "Context-Aware Cloud Robotics for Material Handling in Cognitive Industrial Internet of Things", *IEEE Internet of Things Journal*, Vol. 5, No. 4, pp. 2272-2281, 2017.

[8] S.S.M. Ajibade, N. Adhikari and D.L. Ngo-Hoang, "An Analysis of Social Networking for E-learning in Institutions of Higher Learning using Perceived Ease of use and Perceived Usefulness", *Journal of Scientometric Research*, Vol. 11, No. 2, pp. 246-253, 2022.

[9] M.H. Masud and X. Huang, "An E-Learning System Architecture based on Cloud Computing", *International Journal of Information and Communication Engineering*, Vol. 6, No. 2, pp. 255-259, 2012.

[10] N. Zanoon and S.M. Khwaldeh, "Cloud Computing and Big Data is there a Relation Between the Two: A Study", *International Journal of Applied Engineering Research*, Vol. 12, No. 17, pp. 6970-6982, 2017.

[11] B. Lin, F. Zhu and J.L. Mauri, "A Time-Driven Data Placement Strategy for a Scientific Workflow Combining Edge Computing and Cloud Computing", *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 7, pp. 4254-4265, 2019.