IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15353

AWS CloudTrail for Monitoring Docker Container Activity

PRATEESH S[1], Mr. S. S. Saravana Kumar[2]

III BCA, Department of Computer Applications, Sri Ramakrishna College of Arts & Science (Autonomous),

Coimbatore – 641006, Tamil Nadu, India[1]

Assistance Professor, Department of Computer Applications,

Sri Ramakrishna College of Arts & Science (Autonomous), Coimbatore – 641006, Tamil Nadu, India[2]

Abstract: With the rapid adoption of containerization technologies such as Docker, monitoring container activity and maintaining security has become an important concern in modern cloud environments. This paper proposes a monitoring framework using Amazon Web Services (AWS) CloudTrail to track and analyze Docker container activity. AWS CloudTrail records API calls and user activities across AWS infrastructure, enabling administrators to monitor system operations, detect anomalies, and ensure compliance. The proposed system integrates Docker container deployment on AWS infrastructure with CloudTrail logging mechanisms to capture container-related events and activities. The collected logs can be stored, analyzed, and visualized to provide insights into container behavior, security incidents, and operational performance. This approach enhances transparency and accountability in containerized environments and supports effective auditing and security management.

I. INTRODUCTION

Containerization has become a popular approach for deploying and managing applications because it allows developers to package applications with their dependencies in a lightweight and portable format. Docker is one of the most widely used container platforms that enables rapid deployment and scalability of applications. However, as the number of containers increases, monitoring their activities becomes a challenging task.

In cloud-based environments such as Amazon Web Services (AWS), it is essential to track system events and maintain logs for auditing and security purposes. AWS CloudTrail provides detailed event logs that capture all API calls made within an AWS account. By integrating Docker container activity with CloudTrail logging, organizations can gain better visibility into container operations, detect suspicious behavior, and ensure compliance with security policies.

This project focuses on implementing a monitoring solution using AWS CloudTrail to observe Docker container activity. The system captures logs related to container operations and provides a centralized monitoring mechanism to analyze system behavior and maintain security.

II. OBJECTIVES AND CHALLENGES

Objectives:
- To monitor Docker container activities using AWS CloudTrail.
- To record and analyze API calls related to container deployment and management.
- To improve security and auditing capabilities in containerized cloud environments.
- To provide centralized logging and monitoring for system administrators.

Challenges:
- Managing large volumes of log data generated by container operations.
- Ensuring real-time monitoring and timely detection of suspicious activities.
- Integrating Docker container events with AWS logging services.
- Maintaining performance while continuously collecting and analyzing logs.

Enhance Security Monitoring:
To continuously monitor container-related activities and detect unauthorized access or suspicious operations within the cloud environment.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15353

Maintain Detailed Audit Trails:
To maintain a complete record of all API calls and system actions performed on Docker containers for auditing and compliance purposes.

Improve System Transparency:
To provide clear visibility into container operations such as creation, deployment, modification, and deletion.

Enable Log-Based Analysis:
To analyze collected logs in order to identify patterns, anomalies, or unusual behavior in container activities.

Support Compliance Requirements:
To ensure that system activities meet security and regulatory standards by maintaining detailed activity records.

Centralized Monitoring System:
To integrate container monitoring into a centralized cloud monitoring platform using AWS services.

Improve Incident Investigation:
To help administrators quickly investigate security incidents using recorded CloudTrail logs.

Optimize Resource Management:
To monitor container resource usage and operational activities for better infrastructure management.

III. SYSTEM ARCHITECTURE

The proposed system architecture consists of Docker containers deployed on AWS infrastructure such as EC2 instances. AWS CloudTrail is enabled to capture all API calls and system activities related to container management.
The architecture includes the following components:

1. Docker Engine – Used to create and manage containers running application services.
2. AWS EC2 Instance – Hosts the Docker environment where containers are executed.
3. AWS CloudTrail – Captures and records API calls and system activities related to container operations.
4. Amazon S3 – Stores CloudTrail log files for long-term analysis and auditing.
5. Monitoring and Analysis Tools – Used to visualize and analyze log data for detecting anomalies and monitoring system performance.

This architecture provides a secure and scalable monitoring solution for containerized applications.

IV. IMPLEMENTATION

The implementation of the proposed system begins with setting up an AWS environment and launching an EC2 instance. Docker is installed on the instance to enable container-based application deployment.

Next, AWS CloudTrail is configured to record all API activities within the AWS account. CloudTrail logs are directed to an Amazon S3 bucket where they are securely stored. Whenever Docker containers are created, started, stopped, or removed, the related AWS API calls are recorded in CloudTrail logs.

These logs can then be analyzed using log monitoring tools or AWS services such as Amazon CloudWatch to identify unusual activities or potential security threats. The system allows administrators to track container operations and maintain a comprehensive audit trail of all system activities.

V. RESULTS AND DISCUSSION

The implementation demonstrates that AWS CloudTrail effectively records and stores detailed logs of container-related activities performed within the AWS environment. The monitoring framework provides visibility into operations such as container creation, deployment, modification, and termination.

By analyzing these logs, administrators can identify abnormal patterns or unauthorized access attempts. The centralized logging system improves the ability to troubleshoot system issues and ensures that all operational activities are properly documented. The results indicate that integrating Docker monitoring with AWS CloudTrail significantly enhances system transparency and security management.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 3, March 2026

DOI: 10.17148/IJARCCE.2026.15353

VI. CONCLUSION

This project presents a monitoring framework that integrates Docker container environments with AWS CloudTrail to capture and analyze container activities. The proposed system improves security, transparency, and auditing capabilities in cloud-based container infrastructures. By leveraging AWS logging services, administrators can monitor system behavior, detect potential threats, and maintain compliance with security policies. The solution provides a reliable approach for managing and monitoring modern containerized applications deployed in cloud environments.

VII. FUTURE ENHANCEMENT

Future improvements to this system may include integrating real-time alerting mechanisms using Amazon CloudWatch alarms to notify administrators about suspicious activities. Machine learning techniques could also be applied to log data to detect anomalies automatically. Additionally, visualization dashboards could be developed to provide a more user-friendly interface for analyzing container activity logs. The system can also be extended to support monitoring across multiple cloud environments for improved scalability.

REFERENCES

[1]. Docker Documentation – https://docs.docker.com/
[2]. AWS CloudTrail Documentation – https://docs.aws.amazon.com/cloudtrail/
[3]. Amazon EC2 Documentation – https://docs.aws.amazon.com/ec2/
[4]. Amazon S3 Documentation – https://docs.aws.amazon.com/s3/
[5]. Merkel, Dirk. "Docker: Lightweight Linux Containers for Consistent Development and Deployment." Linux Journal.