International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 6208-6223
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Leveraging AWS CloudWatch, Nagios, and Splunk for Real-Time Cloud Observability

Naga Murali Krishna Koneru*

Hexaware Technologies Inc, USA
* **Corresponding Author Email:** nagamuralikoneru@gmail.com - **ORCID:** 0000-0002-5247-7853

Article Info:

DOI: 10.22399/ijcesen.3781
Received : 05 June 2025
Accepted : 19 Auguat 2025

Keywords

Cloud Infrastructure Monitoring,
AWS CloudWatch,
Nagios, Splunk,
Real-Time Monitoring,
Cloud Performance,
Machine Learning

Abstract:

The article examines the importance of monitoring cloud infrastructure and capabilities of AWS CloudWatch, Nagios and Splunk in providing real-time views of operations. According to the survey of enterprises that are shifting toward flexible, scalable and economical cloud architecture, there is a need to ensure consistent performance, availability, and security of cloud workloads. Such continuous, real-time monitoring allow proactive notification and corrective actioning of performance bottlenecks, security incidents and service downages, prior to their access to end-users. The paper will analyze the functional scope and architectural strength of every tool and the deployment constraints of each tool. The AWS CloudWatch is highly integrated with AWS services and has a broad level of metrics and automated alarms and log analytics on cloud-native workloads. Being an open-source solution, Nagios allows configuration of its monitoring capabilities and an easy integration with hybrid and multi-cloud platforms. Splunk has proven to be feasible because it has high rates of real-time log ingestion, ability to conduct advanced analytics, and predictive modeling using built-in machine learning algorithms. Comparative analysis draws attention to the fact that, despite certain similarities, each of the platforms can serve the various observed strategies, which enables organizations to choose an effective monitoring stack based on their cloud service model. The paper is also focused on best practices: standardization of metrics, anomaly detection, and alert optimization, and emergent trends, such as self-healing infrastructure and observability pipelines with AI. With the strategic monitoring and the usage of tool specific features, organizations are able to achieve operational resilience, high availability, and compliance readiness in the new age cloud based context.

1. Introduction

Using cloud services has become key for leading businesses since they are flexible, scalable, and cheaper for computing, storage, and networking. As more organizations put their vital applications and services in the cloud, it has become more important than ever to maintain their performance, safety, and accessibility. Cloud infrastructure monitoring means constantly monitoring and handling the condition and use of cloud resources. Being able to monitor effectively helps organizations react to dangers early, use their assets wisely, and guarantee that services continue working efficiently. It is essential to have instant insights into cloud settings since resources in the cloud are always flexible and changing. Unlike regular in-house systems, capacity in the cloud can increase or decrease when needed. Flexibility creates problems that make it tough to predict the system's actions and ensure it performs typically well. WATCHING in real-time allows organizations to watch over their cloud environments and notice any issues instantly to respond immediately before problems reach users. Observing cloud infrastructure live allows IT teams to decide what to do based on facts, deal with problems efficiently, and distribute resources wisely. Various tools now help companies keep track of their cloud infrastructure. AWS CloudWatch, Nagios, and Splunk are particularly popular and used by many because they have strong monitoring capabilities. CloudWatch is an AWS tool designed to help check how AWS cloud resources are operating. It gathers and follows up on important metrics, looks through log files, and gives users immediate notification through alarms if there is drop-in performance or unusual occurrences. The strong integration among AWS services offered by

CloudWatch makes it especially valuable for using AWS.

Unlike the others, Nagios is a free tool prized for its many capabilities and ability to adjust to different scenarios. It can check both cloud infrastructure and traditional systems, networks, and apps. Users can create their own checks and alerts in Nagios, which makes it ideal for dealing with complicated, hybrid cloud environments. With plugins, users can add monitoring for many different systems and services to Grafana. Using Splunk to review and learn from cloud machine data, such as logs and performance statistics, is also possible. In contrast to AWS CloudWatch, which only works with AWS, Splunk allows the addition of different cloud platforms and in-house hardware to its network. It allows organizations to analyze data as it arrives and gather insights from a lot of log and event data. Splunk's powerful search features and machine learning tools allow users to spot issues, deal with them, and make important predictions. This article shows how to use AWS CloudWatch, Nagios, and Splunk to monitor cloud infrastructure. The lessons will explain each tool's operation, strengths, weaknesses, and ways they can help provide up-to-date knowledge about cloud infrastructures. Besides, the article will help in choosing the best tool for each monitoring task and offer tips for improving monitoring strategies on today's cloud systems. At the close of this article, readers will know why cloud monitoring is necessary and how to use these tools to keep their cloud-based applications and services running smoothly.

2. Understanding Cloud Infrastructure Monitoring

Cloud infrastructure monitoring means continuously checking the availability, performance, and safety of cloud services. Using different system metrics and logs, cloud platform operations can be understood. Today, cloud infrastructure allows IT departments to expand, adapt, and save money. As a result, monitoring cloud services is necessary to assess if they satisfy business needs by working efficiently and remaining secure. To ensure cloud systems perform well, it is essential to continuously measure the key metrics that come with cloud infrastructure monitoring. A broad range of metrics falls into these three main categories: performance, availability, and security. Performance metrics are used to monitor cloud resources, including CPU activity, memory usage, access to storage, and network traffic speed. Administrators review these metrics to identify potential issues with certain services and address them with additional resources or improved configurations. Availability metrics track cloud services' uptime to ensure that applications and services remain uninterrupted for users. Services like Amazon CloudWatch continuously monitor these services, and when an organization’s availability thresholds are exceeded, they trigger alerts or corrective actions. Additionally, monitoring access logs, user behavior, and network traffic helps to identify any unauthorized access or potential security threats. Ensuring data security is vital in the cloud because much of the data is exchanged over public networks (Chavan, 2024).

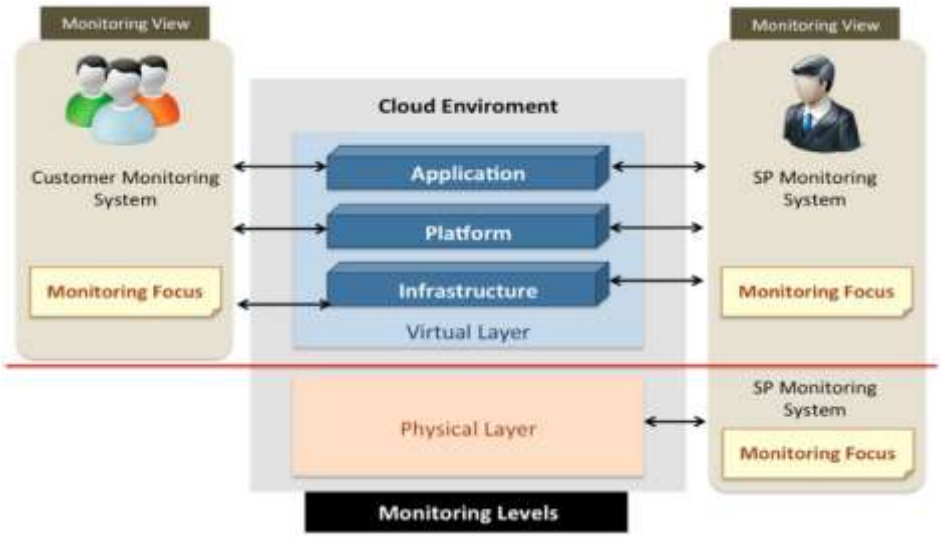

Figure 1: *Cloud monitoring structure*

At the same time, there are significant hurdles when monitoring cloud infrastructure. One of the most significant problems with clouds is their flexibility and changeability. Unlike standard on-premise solutions, cloud services can adjust their size automatically, making monitoring the infrastructure a challenge. Multi-tenant cloud architecture also means that many users can access available

resources simultaneously, which presents challenges to keeping an eye on performance without affecting their security or privacy. There is even more complexity due to all the data cloud systems constantly generating. These tools must review and make sense of all the information immediately while keeping administrators from being overloaded with too much data. Monitoring the cloud through real-time insights is very important. Thanks to the information, admins can immediately respond to unexpected problems during operations. Taking Action quickly helps lessen the effect of problems on how the service works. AWS CloudWatch, Nagios, and Splunk become helpful for administrators who need to watch over critical metrics and respond quickly to issues or alerts. Watching systems in real-time allows automatic reactions, like scaling up resources, to make sure they are performing as they should. Cloud infrastructure monitoring helps improve cloud services' performance, uninterrupted operation, and security. Using monitoring tools and real-time knowledge, enterprises can make their cloud systems work well and always be secure. Still, managing these environments becomes a problem due to the changes in the cloud and the enormous amount of data, so it is important to use updated monitoring techniques. As technology in the cloud progresses, increasing emphasis on good monitoring makes it mandatory for organizations to stay current (Aceto et al, 2013).

3. Key Tools for Cloud Infrastructure Monitoring

Managing cloud infrastructure is vital so that systems operate at their best, stay up, and fix issues before they cause trouble. Many people use AWS CloudWatch, Nagios, and Splunk as popular tools for monitoring cloud infrastructure. Because every tool has specific strengths, they are suited for specific uses in cloud infrastructure monitoring.

3.1 Introduction to AWS CloudWatch, Nagios, and Splunk.

AWS CloudWatch provides complete monitoring through AWS and allows users to monitor the performance of their cloud applications and resources instantly. It comes with information and alarms so users can check the status of their infrastructure in Amazon Web Services. Thanks to its integration with AWS, CloudWatch can keep an eye on EC2 instances, RDS databases, and Lambda functions. Nagios is free software that many organizations use to monitor their systems on both local servers and in cloud environments. It is centered around monitoring servers, switches, applications, and services. Prometheus can be set up in many ways and monitors local systems and those running in the cloud. Nagios does a great job of providing detailed monitoring reports and warnings about failures and lagging performance. Splunk supports searching, watching, and analyzing machine-produced data in real-time. While it can be used for many jobs, it excels at managing logs and correlating events. Since Splunk allows businesses to study large amounts of data, it is vital for finding patterns and solving complex problems in the cloud (Zadrozny & Kodali, 2013).

3.2 Comparison of the Tools Features

AWS CloudWatch

Companies already part of the AWS ecosystem should find AWS CloudWatch very convenient since it works closely with other AWS services. Using this feature, information can be gathered from multiple AWS services and statistics such as CPU load, I/O disk, and network data can be closely checked. Users can set custom alarms using CloudWatch to respond to specific events automatically. Additionally, CloudWatch Logs allows monitoring and diagnosing application logs, allowing administrators to notice when their application operates slowly by consuming more resources. A significant advantage of AWS CloudWatch is its ease of scaling. CloudWatch can easily manage more information as a company expands, so the monitoring stays up-to-date. AWS Lambda is also fully integrated with CloudWatch, making the service highly flexible for quick and constant monitoring (Chavan, 2021).

Nagios

Nagios is famous for being both versatile and powerful. Because it is open source, people can configure the monitoring system as they see fit, which helps it handle different environments, including on-premises and cloud sets. Because Nagios can monitor anything from servers to networks to databases and applications, it makes a valuable addition to any mixed environment. Its primary advantage comes from the way it alerts users. Should predefined thresholds become exceeded, it instantly sends notifications and summarizes the issue completely. Unlike AWS CloudWatch and Splunk, more manual setup is needed with Nagios when integrating with different cloud platforms and systems. Even so, it helps companies get monitoring with fine details for various parts of their infrastructure at an affordable price.

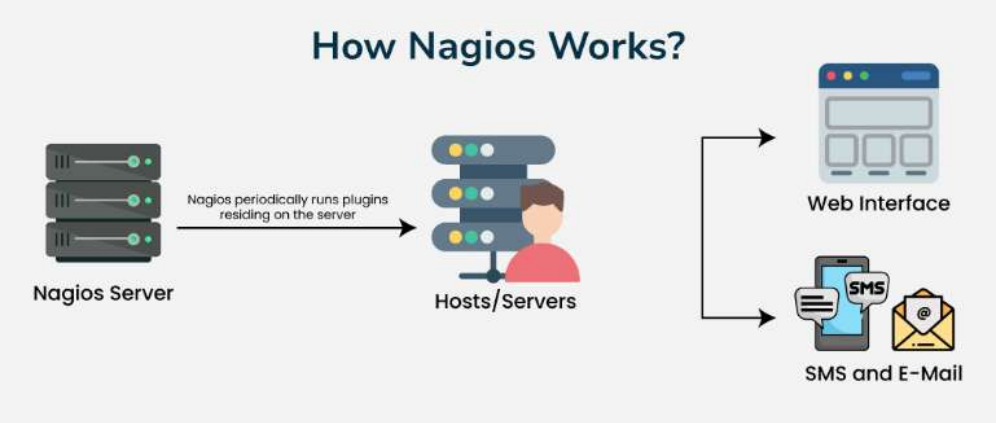

Figure 2: *Complete Tutorial of What is Nagios Splunk*

With advanced analytics tools, Splunk is effective for analyzing how big cloud environments are performing (Liu et al, 2019). This solution is best for organizations that have to gather and study extensive logs from multiple areas, such as the cloud, applications, and security systems. Splunk's power to monitor log files makes it ideal for spotting security issues, performance problems, and areas where operations can be improved. Splunk's user interface is intuitive and straightforward. Using dashboards, users can immediately see the trends and exceptions in their data. Moreover, Splunk allows working with many third-party tools to monitor more complicated systems. However, not all organizations can afford to use the technology due to its high cost.

4. AWS CloudWatch: The AWS Native Monitoring Solution

AWS CloudWatch offers Amazon Web Services (AWS) users a service to monitor their applications, infrastructures, and services. With CloudWatch, users can monitor, track, and measure data, check through logs, and manage alarms in an integrated interface. Real-time access to cloud resources, applications, and services makes this solution important for overseeing and improving cloud environments. Businesses using cloud technologies for efficiency greatly benefit from AWS CloudWatch, which ensures that their systems perform well and without fail (Konneru, 2021).

4.1 Key Features of AWS CloudWatch

Many important features make CloudWatch a dependable tool for monitoring cloud infrastructure and applications. Because of these features, it is possible to monitor AWS resources in real-time and gain valuable insights.

Metris Collection and Storing

CloudWatch can collect metrics from EC2 instances, RDS databases, Lambda functions, and several other AWS services. Individuals monitor the CPU, memory usage, disk activity, network performance, and similar indicators. CloudWatch gathers these metrics at set intervals and holds onto them for users to review and analyze future trends. Obtaining the data helps spot areas of poor resource use, optimize system aspects, and solve problems before they cause significant trouble.

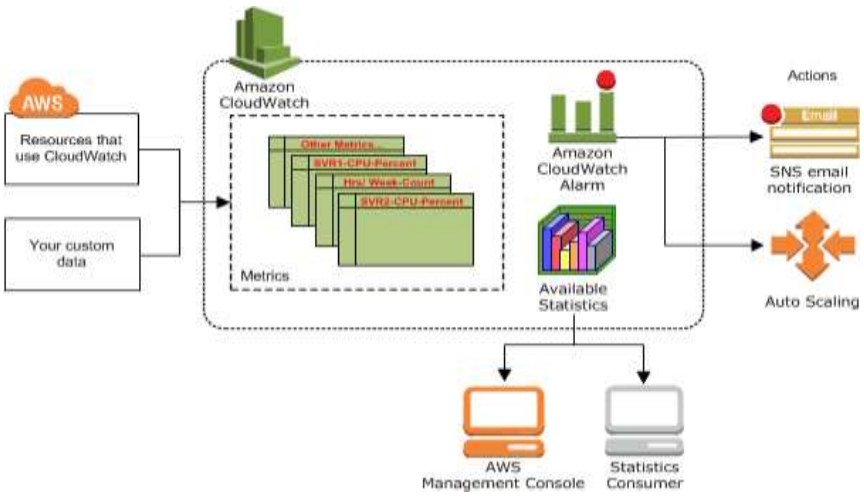

Figure 3: *A Comprehensive Guide to AWS Cloudwatch Monitoring*

Alarming and Notification

An important part of CloudWatch is that it allows setting alarms when specific issues occur (Pourmajidi et al, 2018). Customers are allowed to set their thresholds in CloudWatch, and if these values are surpassed or go below, alarms will be triggered automatically. For instance, an alert is sent to the relevant team if the CPU works above 80% daily for over two hours. CloudWatch works with SNS (Simple Notification Service) to quickly deliver notifications by email, SMS, or other means so that problems do not go unnoticed. Through alarm and notification systems, organizations can learn about upcoming problems quickly and quickly respond to minimize downtime.

Log Monitoring and Management

It contains advanced tools for tracking log data in the cloud. Using CloudWatch Logs, people can retrieve log information from various AWS resources and apps. Real-time streaming of these logs means users can view application mistakes, system performance issues, and safety events as they happen. CloudWatch Logs allows for filtering and searching of logs, simplifying the analysis of specific events or the resolution of issues. Logs are managed centrally using the service, which aids in tracking them across all instances, services, and regions.

Dashboards and Visualization

With CloudWatch, personalized dashboards can be built to view metrics, alarms, and logs graphically (Lingamallu & Oliveira, 2023). These dashboards provide a visual representation of cloud infrastructure performance. Graphs, charts, and tables in CloudWatch Dashboards display key performance indicators in real time. The graphs and charts help identify problematic or unusual information with ease. Dashboards enable team members to monitor and make decisions on data collaboratively.

4.2 How AWS CloudWatch Integrates with other AWS Services

CloudWatch is recognized as vital within the AWS ecosystem because AWS services work together so seamlessly. CloudWatch integrates with AWS Auto Scaling to begin scaling instances after set limits are reached. When the demand for an application increase, CloudWatch monitors the resources and automatically adds more EC2 instances to ensure the application continues functioning smoothly. It is also possible for CloudWatch to automatically send notifications or execute selected scripts in the AWS Lambda service when an alarm is triggered. By using CloudWatch with AWS Systems Manager, operations can be automated, and current data can be leveraged to reduce resource waste. Integration enhances the management of AWS resources and ensures the infrastructure operates efficiently (Poornalinga & Rajkumar, 2016).

4.3 Real-Life Use Cases and Applications of AWS CloudWatch

CloudWatch is used by several industries to keep an eye on cloud infrastructure and applications. In web commerce, CloudWatch is often used to view web server results, follow customer trends, and catch early signs of breakdowns. If website latency exceeds the set limit, CloudWatch can cause an alarm to be raised so operations can address the problem. In finances, CloudWatch is relied on to monitor transactional systems and find out any issues or signs of breaches. When working with IoT applications, CloudWatch allows monitoring of devices and sensors, and the collected real-time data helps optimize performance and detect upcoming maintenance (Stephen et al, 2019). They prove that AWS CloudWatch can be used in multiple situations to handle various tasks efficiently.

4.4 Best Practices for Using AWS CloudWatch in Cloud Monitoring

Organizations should follow specific best practices for better results with AWS CloudWatch. It is most important to create custom metrics that match the business's precise needs. While CloudWatch provides access to predefined metrics, adding custom metrics allows for checking performance details. Careful consideration should be given when setting up alarms. A flood of alerts can make it difficult to notice errors, while very few alerts can cause important issues to be missed. Alarms should be used only for essential items that need immediate attention. Additionally, frequently checking and studying the CloudWatch logs can help discover common issues. With CloudWatch, automated actions can be set up to improve how server issues are addressed. CloudWatch Dashboards offer a straightforward way to track performance metrics and promptly detect any problems, which is crucial for swift problem resolution (Nikkhouy, 2016).

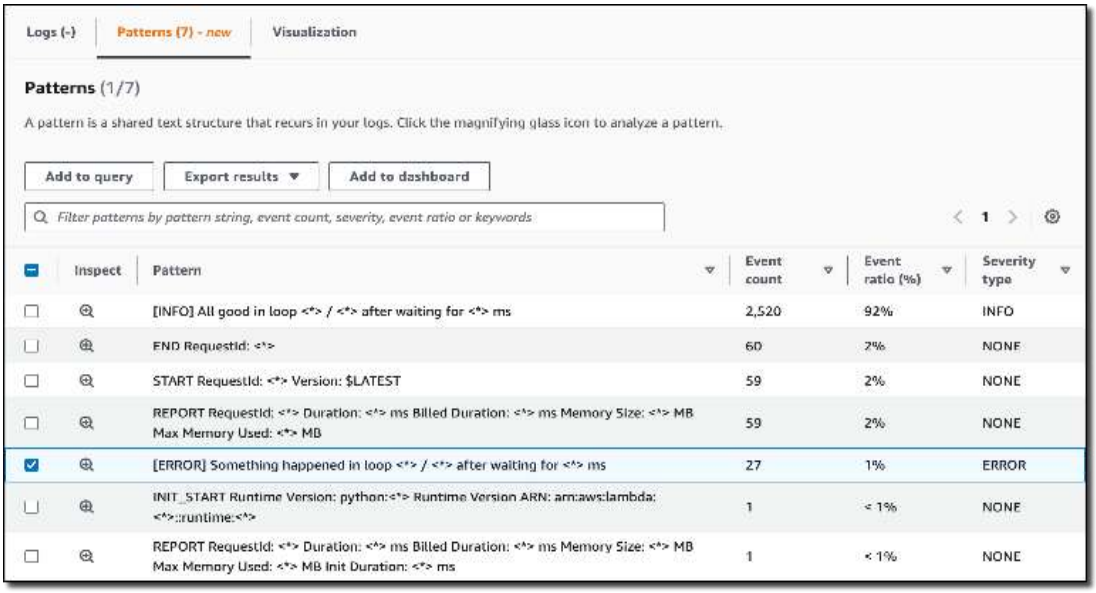

Figure 4: *Amazon CloudWatch Logs now offers automated pattern analytics and anomaly detection*

5. Nagios: Open-Source Monitoring for Flexibility

Depending on Nagios, it is a wise choice as it offers an exhaustive overview of cloud performance. Because Nagios is easily customized and has many plugins, it lets organizations watch over their cloud networks, devices, and servers in real time. Because Nagios monitors proactively, businesses have enough time to address system problems before they turn into issues that shut down the system. Nagios helps maintain the health of the cloud infrastructure. Created in 2002, Nagios rose to lasting popularity and is now regarded as a central open-source system for network monitoring. Monitoring's main job is to monitor systems, applications, and the network's infrastructure. Throughout its history, Nagios has become adaptable to many purposes, supporting cloud infrastructure monitoring as one of its main features (Barth, 2008). Since Nagios is very customizable, it works for organizations of all sizes. Thanks to its open-source code, users can adjust and build upon CloudWatch to meet their own needs in cloud monitoring.

5.1 Features and Capabilities of Nagios for Cloud Infrastructure

Nagios has the features needed to monitor cloud platforms effectively. The most important features are monitoring both hosts and services, providing alerts, and the plugin system.

Host and Service Monitoring

Nagios works best when it tracks hosts and the services running on them. Tracking these types of devices as part of monitoring includes servers, virtual machines, and network nodes. Nagios can watch over the hardware and software resources in a cloud environment. It keeps track of performance by monitoring uptime, checking usage of resources, network performance, and much more, and providing in-depth details about servers and services. Plugins designed for their architecture monitor databases, web servers, and load balancers in the cloud (Lee et al, 2021).

Alerting and Reporting

It can send advanced warnings when anything needs attention. Once a problem arises, whether it involves decaying performance, loss of uptime, or a network error, Nagios sends messages through email, SMS, or various other forms of communication. They allow system administrators to act swiftly when a problem is detected. In addition, Nagios produces detailed reports on how the system works, which can be used to study how it worked in the past and plan for its future use. Infrastructure health and trends can be seen through reports customized to meet specific needs.

Plugin Architecture and Extensibility

A strong point of Nagios is that its plugin architecture allows users to increase its capabilities. Nagios can work with many plugins that keep track of various systems, applications, and cloud services. Because Nagios is flexible, it can handle AWS, Google Cloud, and Microsoft Azure monitoring. Users can also make plugins to supervise services or devices not included in the default support. The flexibility of Logstash is more useful than AWS CloudWatch, which may still require users to configure extra tools or setups for specialized tasks (Sardana, 2022).

5.2 Nagios vs. AWS CloudWatch

Even though Nagios and AWS CloudWatch are often chosen to monitor the cloud, they have important differences. Since it is integrated with other AWS services, AWS CloudWatch provides an easy way to monitor EC2, Lambda, and RDS resources. It collects extensive information and records from AWS offerings, and this data is especially valued by users who are deeply involved with AWS. However, CloudWatch is not as flexible as Nagios when used with resources outside of AWS or custom services. Nagios does not depend on one cloud provider, making it usable in mixed cloud environments. Because Nagios is flexible, companies can monitor everything on all platforms, including AWS, Google Cloud, and their premises. Besides being an open-source project, Nagios can be customized and works well with third-party products. However, since Nagios requires more user configuration than AWS CloudWatch, it might be difficult for teams with little or no detailed monitoring experience (Ward & Barker, (2014).

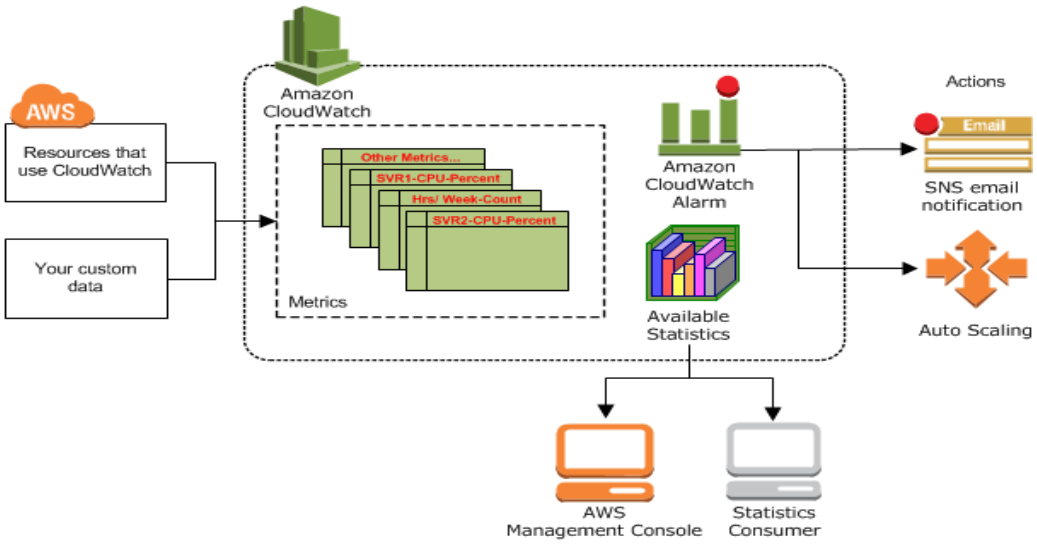

Figure 5: *Amazon CloudWatch vs Nagios for Cloud Infrastructure Monitoring*

5.3 Preparing Nagios for Cloud Monitoring

To use Nagios to monitor cloud platforms, several steps must be followed. First, Nagios must be installed on a functioning server, after which the Nagios Core software and any additional plugins are installed. Following the installation, hosts and services are listed in Nagios configuration files, specifying which systems to monitor. When using Nagios in the cloud, plugins created for AWS EC2, RDS, and the S3 service can be accessed. Nagios integrates with cloud services and application APIs to detect resources in the cloud. For example, it can be configured to monitor auto-scaling groups in AWS, adjusting its monitoring scope as new or old instances are created. Once set up, Nagios collects logs, generates alerts, and provides reports based on predefined thresholds (Mongkolluksamee et al, 2010).

5.4 Best Practices and Use Cases for Nagios

Some best practices should be used to ensure Nagios performs optimally in cloud infrastructure monitoring. First, it is important to set reasonable goals for what needs to be monitored. If thresholds are set too high, excessive false alarms may occur; if they are set too low, some issues might go undetected. Regularly updating Nagios and its plugins will enhance their compatibility with current cloud systems. Many businesses today rely on multiple cloud providers, and Nagios supports monitoring resources across each platform. Due to its plugin-based design, Nagios is particularly well-suited for businesses that must address specialized or custom requirements. For instance, when businesses have legacy systems operating alongside cloud services, Nagios can integrate all monitoring efforts into a unified solution (Verginadis, 2023).

6. Splunk: Powerful Data Analytics for Cloud Monitoring

For today's cloud-focused services, checking the infrastructure is necessary to help achieve strong performance, safety, and always-on service. Organizations often rely on Splunk for operational intelligence to quickly see what is happening in their cloud infrastructure. Thanks to Splunk, users can watch important system logs, oversee performance metrics, and use predictive features to tackle problems and prevent them from causing issues with the business. Handling a lot of unstructured data makes Splunk particularly helpful for cloud

infrastructure, where both the speed and complexity need solutions to keep up.

Figure 6: *Splunk Infrastructure Monitoring*

6.1 Features and Capabilities of Splunk

Splunk has several important features for monitoring organization's cloud infrastructure. These include collecting data instantly, gathering logs, carrying out advanced data analysis, using machine learning, creating personalized dashboards, and sending alerts. One of Splunk's main strengths is collecting data as it happens in real time. It monitors the cloud by regularly checking data from application logs, system logs, and network performance. As a result, cloud infrastructure administrators can always quickly identify issues when they arise. Splunk can quickly manage large amounts of incoming data, meaning teams can act fast when something happens in the system (Sardana, 2022). Almost every web server, database, and application on the cloud generates logs that must be aggregated and viewed regularly.

Splunk brings all logs together in one place, allowing teams to review them and identify problems more easily. By connecting logs from various sources, Splunk helps discover difficult-to-see trends. Gathering all relevant information in one location reduces the time required to find it, enabling quicker incident handling. Using advanced analytics and machine learning, Splunk monitors trends, issues, and potential risks in the cloud. Machine learning helps Splunk determine if a system is about to fail, detect unusual user actions, and identify security issues. Early warnings are provided, enhancing reliability and security. Additionally, Splunk assists in investigating the causes of performance issues and allows prompt action to resolve them. Splunk also enables the customization of dashboards and alerts to meet specific needs. Dashboards can be tailored to monitor key infrastructure details, such as CPU usage, network updates, and application response times. Furthermore, custom alerts can be created using threshold limits to quickly notify teams of suspicious activities (Sommer, 1999). Alerts are sent promptly via email or SMS messages.

6.2 How Splunk Compares with AWS CloudWatch and Nagios

All these platforms help monitor cloud infrastructure and have different features designed to suit various types of organizations. With AWS CloudWatch, basic statistics on AWS resources can be viewed, log information can be combined, and monitoring alerts can be set up. However, it cannot perform all the functions that Splunk can, which can pull in data from a broader range of sources, making it valuable for hybrid or multi-cloud setups. Nagios, by contrast, is an open-source package that performs standard host and service monitoring. It provides precise data about the availability, speed, and health of Hyper-V systems. However, Nagios does not offer advanced analytics and machine learning, which Splunk can deliver. Although Nagios is suitable for basic use, Splunk's powerful features enable organizations to leverage vast data, look ahead with analytics, and gain clearer insights (Solis Patrón, 2015).

6.3 Setting Up and Using Splunk for Cloud Infrastructure Monitoring

In order to monitor cloud infrastructures with Splunk, it must be integrated with various cloud services, applications, and data sources. First, install the Splunk Universal Forwarder, a lightweight program that gathers logging and metrics from the cloud. After installation, information from Amazon Web Services (AWS), Microsoft Azure, or Google Cloud can be set up to deliver logs and metrics to Splunk. After the data is in Splunk, people can work with dashboards, run custom searches, and arrange for alerts depending on the set rules. For

organizations that combine multiple cloud services, Splunk ensures monitoring of all environments by collecting data from the cloud and teaming up with additional tools (Barker, 2020). Having one system in place allows organizations to check that no area of their network goes unmonitored.

6.4 Best Practices and Use Cases for Splunk

Splunk supports numerous situations, such as monitoring performance and finding security threats. Following a few guidelines on Splunk can help achieve better monitoring results on cloud-based systems. When all logs are in one location, they can be analyzed, monitored, and secured simultaneously. Using Splunk, technicians can quickly find and analyze logs live, saving much time in resolving technical issues. Splunk's machine learning allows security teams to find and resolve unexpected events or security threats before they cause problems. Using Splunk, unauthorized access, data breaches, and other dangerous events can be discovered and stopped in real time. Monitoring key metrics and system indicators allows organizations to improve the performance of their cloud infrastructure. Real-time data analytics in Splunk helps teams find bottlenecks, set up systems more effectively, and divide resources so the system works at its best (Raj et al, 2015).

7. Comparison of AWS CloudWatch, Nagios, and Splunk

The cloud industry uses AWS CloudWatch, Nagios, and Splunk to keep systems running smoothly, securely, and without issues. Because of their specific functions, each tool serves different needs in different cloud situations. The article examines the most important aspects of these tools, such as when each should be selected, the costs, and the positives and negatives associated with each.

7.1 AWS CloudWatch

AWS CloudWatch is designed to help monitor apps running in the AWS environment. It ensures complete watch over AWS products, including EC2, Lambda, and S3. CloudWatch gathers and follows metrics, logs, and events to provide real-time updates on how AWS systems are running. With Metric Alerts, users can set up responses automatically, which has become vital for cloud-native apps.

Pros:

- A simple flow to add AWS features to the application.
- Manages and scales up resources automatically when they are needed.
- Presents significant statistics and logs from AWS systems.

Cons:

- Non-AWS infrastructure is not fully supported.
- Using more log and custom metrics can be costly.

AWS CloudWatch is mainly helpful for companies that heavily use AWS services. It should be used for AWS workloads and environments. The price varies based on incoming data, custom metrics, and alarms triggered, so costs increase as the infrastructure size increases (Singh, 2022).

7.2 Nagios

Many people praise Nagios because it is open-source and easy to customize. The system allows users to oversee cloud and local infrastructure and use many plugins to monitor servers, networks, and databases. Organizations can also adjust the tool to meet their own needs.

Pros:

- Plugins allow to customize a website in many different ways.
- Because it is free and open-source, using it is affordable.
- One can keep an eye on both systems located on-site and those in the cloud.

Cons:

- It can sometimes be challenging to get started and maintain.
- Only a small amount of real-time analytics is available.
- Monitors require extra setup for each cloud platform supported.

It is an excellent fit for businesses that must cover multiple platforms and know how to set up and manage Nagios (Josephsen, 2007). It is made for cloud platforms that include private, public, and community-supported resources. While it is free to use, there may be expenses associated with purchasing the necessary hardware and adjusting it to meet specific needs.

7.3 Splunk

With Splunk, a fully featured analysis tool is provided that enables monitoring and viewing of data in real-time. Whereas AWS CloudWatch is for AWS alone, Splunk monitors multiple cloud platforms, local systems, and blended systems. Splunk stands out because its machine learning tools and advanced analytics let organizations understand vast data, making it ideal for companies that care about strong security, compliance, and managing business activities (Parikh, 2019).

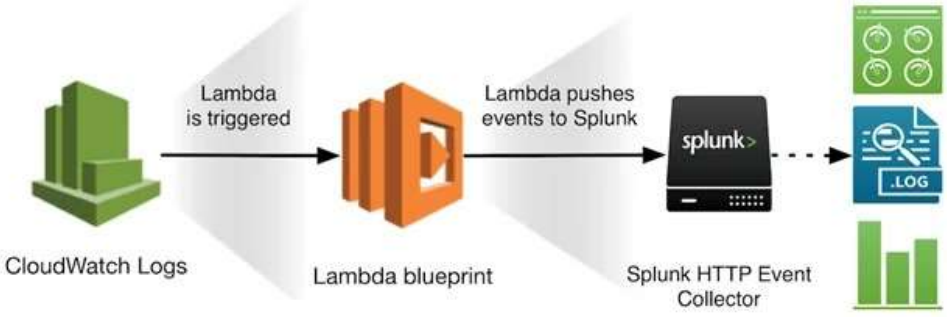

Figure 7: *Monitoring AWS Cloud with Splunk using AWS CloudWatch*

Pros:

- It can run in many settings, including architectures with hybrid and multi-cloud structures.
- Easy-to-use search and data analysis technology.
- Robust reporting and visualization tools are available.

Cons:

- It can become very costly for mass data intake.

Setting up such networks can require plenty of infrastructure, making them extra costly for bigger organizations. There is a lot to learn for the first time using it. Firms in need of sophisticated analytics and log maintenance find Splunk most valuable. Thanks to their ability to share detailed results and reports to identify and fix unusual activities, such systems can maintain security and compliance effectively. The expense, though, can be too much for smaller companies that need to use large amounts of data.

7.4 Cost Comparison

Pricing for AWS CloudWatch, Nagios, and Splunk differs significantly. AWS CloudWatch operates on a pay-as-you-use model, where charges are based on metrics, logs, and alarms. Smaller projects may find it affordable, but costs increase as the load grows. Nagios, being open-source, is free; however, the costs associated with server management and setup still apply. With Splunk, the pricing depends on the amount of data imported, making it more expensive when handling large volumes of logs.

7.5 Integration in Hybrid Solutions

Hybrid solutions combine different monitoring technologies in organizations (Grossi et al, 2017). AWS CloudWatch can be set up to check AWS resources, and Nagios can observe on-premise and infrastructure from third-party clouds. Using Splunk, data from AWS CloudWatch and Nagios can be collected and reported in one place. Thanks to this approach, enterprises can access AWS CloudWatch's cloud-monitoring tools, Nagios for infrastructure supervision, and Splunk for data analysis.

8. Integrating Monitoring Tools for Comprehensive Insights

Now that technologies are more complex, continuously monitoring the infrastructure is necessary for everything to function correctly. Integrating AWS CloudWatch, Nagios, and Splunk helps businesses get detailed, scalable, and robust real-time monitoring information real-time monitoring information about their systems' health, performance, and safety. Alone, the tools are helpful, yet once they are put together, they create a strong and unified system for monitoring.

8.1 Advantages of Relying on AWS CloudWatch, Nagios, and Splunk

AWS CloudWatch is built to track AWS tools and applications, letting users explore metrics and logs about server performance and their applications (Farshchi, et al, 2018). Companies can collect real-time data updates using this service, which is advantageous when working with AWS. Most people use Nagios to watch both in-house and cloud systems, thanks to its detailed capabilities for network monitoring. MONITOR supports various customized settings and can watch over hardware, network services, and applications. Splunk is very good at examining machine information and turning it into meaningful data necessary for SIEM and application performance monitoring. This combination informs how the infrastructure works, how protected it is, and how users behave.

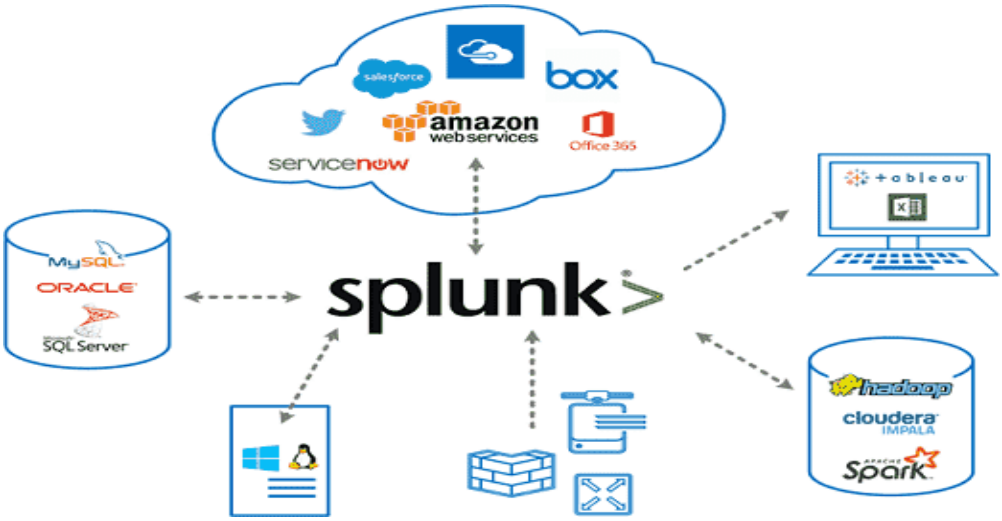

Figure 8: *What Splunk is used for | Splunk SIEM*

8.2 How to Integrate the Tools to Provide Enhanced Monitoring

It is essential to plan how AWS CloudWatch, Nagios, and Splunk are connected to leverage the strengths of each tool. AWS CloudWatch collects log information from AWS resources, while Nagios monitors equipment and infrastructure that AWS does not support by default. With Splunk, organizations can gather data from AWS CloudWatch and Nagios, providing a comprehensive view of the entire infrastructure in one place. Splunk enhances this by allowing users to search, group, and compare logs and event data from different sources (Singh, 2023). AWS CloudWatch tracks statistics for cloud services, such as CPU and memory usage, whereas Nagios monitors the health of on-premise hardware and the performance of the network. Splunk consolidates this data, enabling security teams to better understand potential risks and unusual behavior. Organizations can integrate APIs and data connectors provided by the tools. By using the CloudWatch Logs App for Splunk, CloudWatch metrics can be sent to Splunk, while alerts from Nagios can be directed to Splunk through SNMP traps or the Nagios Splunk Integration.

8.3 Creating a Unified Monitoring Systems

Having one monitoring system makes it manageable to manage logs, metrics, and alerts at once. As a result, all infrastructure data is combined, and operators can see the status of their entire system. An organization may monitor resource usage of EC2 instances using AWS CloudWatch, the health of its servers on-premises with Nagios, and the logs and events produced on both with Splunk. When the tools have been linked, Splunk receives all alerts from CloudWatch and Nagios for live review and understanding. Thanks to this process, IT administrators can proactively address weak performance, security issues, and workload blockages. In addition, with integration, repairing issues becomes less challenging. Should an issue arise, administrators can use Splunk to compare AWS and on-premise logs to determine whether an AWS failure, slow network or crashed server caused it (Méndez Roca, 2020).

8.4 Use Cases and Real-World Scenarios

When dealing with practical issues, such an integrated approach is essential. In e-commerce, CloudWatch can keep an eye on the well-being of AWS-hosted web servers, Nagios can observe network usage and the state of hardware, and Splunk supplies up-to-the-minute insights on customer buying, incidents of hacking, and application effectiveness. Whenever Splunk sees an overload of users, it gathers information from CloudWatch for high CPU usage and Nagios logs for network crowding to help IT teams intervene quickly. For security reasons, Splunk integrates with CloudWatch and Nagios to recognize unusual login attempts, giving a fast response to risks (Al Said, 2016).

9. Research Methodology

The research aims to see whether AWS CloudWatch, Nagios, and Splunk provide real-time input for cloud infrastructure monitoring. Here is a summary of the study design, data collection, and analysis. Researchers used quantitative and qualitative approaches to ensure the selected monitoring tools were fully understood. The study is designed to record individuals' experiences using AWS CloudWatch, Nagios, and Splunk for cloud monitoring and their results.

9.1 Data Collection Methods

Interviews are planned with IT professionals, cloud architects, and system administrators using AWS CloudWatch, Nagios, and Splunk daily in production. Those participating will have experience applying and using these solutions, selected using purposive sampling. The interviews will help to understand the current monitoring functions, benefits and drawbacks, and their contributions to cloud infrastructure management. The interview questions will be prepared in advance, allowing participants to respond fully and ensuring similarity in each interview (Dhanagari, 2024). Apart from conducting interviews, it is important to check industry publications, white papers, and case studies. This review will look at research comparing how well AWS CloudWatch, Nagios, and Splunk perform. Secondary information gives important background and performance insights for the tools used in the evaluation. The study will examine how the monitoring solutions are used in various cloud settings and what the results are, helping to judge their usefulness. Cloud infrastructure teams will be given surveys and polls online to better support the survey. Survey questions will collect numerical data on what AWS CloudWatch, Nagios, and Splunk users think, decide, and prefer. Survey questions will be written to evaluate how users are satisfied, whether the tools are practical, and how dependable they believe they are. The survey's outcomes will be combined and analyzed to compare how the three tools perform in monitoring cloud services.

9.2 Data Analysis

The data collected will be analyzed using both qualitative and quantitative methods. The responses gathered in the interviews will be reviewed to identify common trends, highlighting important information about the effectiveness of the monitoring tools. Thematic analysis will be applied to understand the participants' words and provide valuable insights into the tools' performance. Analysis of survey results will utilize descriptive statistics, including the preparation of frequency tables and the calculation of average scores for each tool. Assessing user satisfaction and the effectiveness of these tools will provide a precise measure for comparing their cloud infrastructure monitoring performance.

	I	J	K	L	M
3	Frequency Table			Descriptive Statistics	
4					
5	Score	Freq		Mean	5.5
6	5.0	1		Standard Error	0.07303
7	5.1	1		Median	5.6
8	5.2	3		Mode	5.7
9	5.5	2		Standard Deviation	0.282843
10	5.6	1		Sample Variance	0.08
11	5.7	4		Kurtosis	-1.31044
12	5.8	3		Skewness	-0.56821
13				Range	0.8
14				Maximum	5.8
15				Minimum	5.0
16				Sum	82.5
17				Count	15
18				Geometric Mean	5.493087
19				Harmonic Mean	5.486055
20				AAD	0.24
21				MAD	0.2
22				IQR	0.5

Figure 9: *Freq Table Descriptive Stats | Real Statistics Using Excel*

9.3 Limitations

It is important to consider some limitations when learning from the research. The study concentrates on three widely used tools for monitoring, AWS CloudWatch, Nagios, and Splunk, and avoids analyzing options that are still new and have not become mainstream. Moreover, because the data collection is done by staff with varying skill levels, some bias could enter the feedback. Someone with relatively low computer skills may evaluate the tools differently from someone with much experience, damaging the reliability of the outcomes (Garland & Noyes, 2004). This research uses different approaches to assess how AWS CloudWatch, Nagios, and Splunk handle real-time monitoring. Applying both types of analysis will help assess the success of the tools for managing cloud infrastructure.

10. Best Practices for Cloud Infrastructure Monitoring

Strong cloud infrastructure monitoring guarantees that cloud systems work well, are accessible, and are safe. Thanks to the dynamic cloud, proper monitoring offers immediate updates, helps manage issues early, and helps companies avoid interruptions. Here are several tips to help

organizations achieve the best results from cloud infrastructure monitoring.

10.1 General Best Practices for Monitoring Cloud Infrastructure

For cloud infrastructure to be efficiently tracked, the team should first decide on specific goals that match the company's objectives. Organizations should monitor important items such as computing, storage, networking, and database resources. Looking at performance indicators—like the use of the CPU, memory, and hard drive storage—helps understand the health of cloud systems. Also, introducing automatic alerts for unusual conditions helps IT teams quickly find and handle problems. Additionally, it is important to set up logging and event tracking properly. Since much data is logged in the cloud, efficient log management is essential to overseeing and resolving issues and supporting cloud infrastructure. Teams can use AWS CloudWatch, Nagios, and Splunk to bring together logs from several systems and create single reports, helping them take Action (Dhanagari, 2024). Businesses can save time and respond to problems more quickly if log analysis is done automatically.

10.2 Security Considerations in Cloud Monitoring.

It is essential to keep cloud infrastructure safe while monitoring it. It is important to include security event monitoring in best practices, such as checking for unauthorized entries and unusual changes to data. Regular monitoring protects against security risks found in cloud resources. Besides, engaging in automated security solutions and joining these with monitoring platforms assures that risks are detected rapidly and that the organization's defense is improved. Services such as AWS GuardDuty, Splunk's SIEM platform, and other security-focused options in the cloud regularly find system vulnerabilities. Security monitoring should be backed by access control to ensure that only authorized users can access specific logs and dashboards (Sandhu & Samarati, 1997). This helps prevent internal attacks, so important information is still safe.

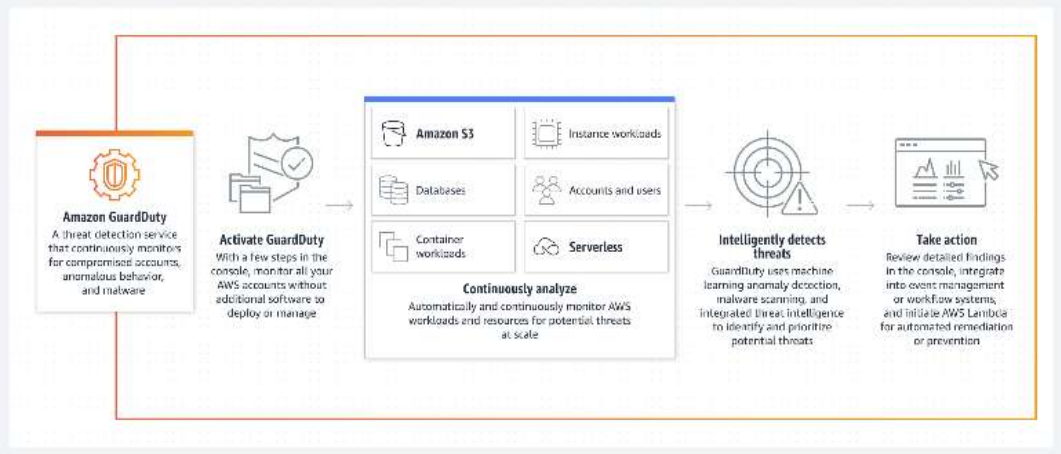

Figure 10: *Intelligent Threat Detection – Amazon GuardDuty – AWS*

10.3 Proactive vs. Reactive Monitoring Strategies

It is generally better to monitor cloud infrastructure in advance than to react to problems as they occur. Continuously checking cloud systems can recognize issues or failures well ahead of user disturbances. Monitoring before problems occur helps companies save resources, pinpoint weaknesses, and reduce upcoming risks. Meanwhile, reactive monitoring steps in when events that are already in progress need to be handled. While resolving issues speeds up when systems are in place, reacting to them can still cause delays, higher costs, and an unpleasant user experience (Galletta et al, 2004). Consequently, primary attention to proactive monitoring plus reactive strategies when things happen is a good way to achieve a strong defense.

10.4 How to Optimize Cloud Performance Using Monitoring Tools

Tools such as AWS CloudWatch, Nagios, and Splunk significantly improve cloud performance by giving insights into system use and actions. AWS CloudWatch allows users to gather and monitor data on EC2 instances and RDS databases and receive real-time information on how all resources run. Using Splunk, businesses can identify changes in cloud performance and security threats within their operations. Relying on monitoring reports to scale automatically can also enhance the cloud's speed and

reliability. AWS Auto Scaling helps organizations change the number of resources they use to match how busy the system is, allowing for the best resource usage. Furthermore, checking performance and analyzing data using AI can help businesses spot where resources are unproductive so they can improve their cloud setup (Weinman, 2012).

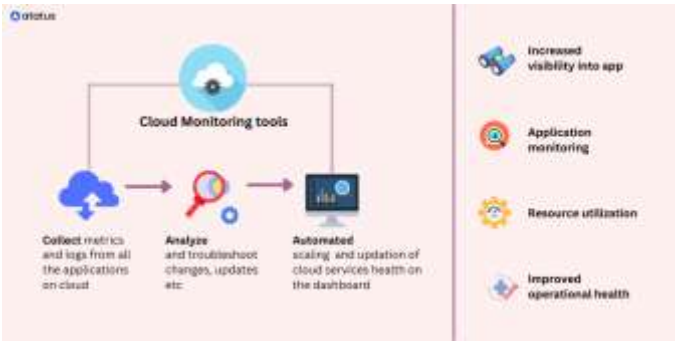

Figure 11: *Cloud Monitoring: A Complete Guide*

11. Conclusion

Monitoring plays a critical role in cloud infrastructure, with tools like AWS CloudWatch, Nagios, and Splunk providing immediate insights into cloud system performance. These tools offer access to essential metrics, enabling organizations to conduct checks, detect suspicious behavior, and respond swiftly to any issues in order to prevent disruptions. Each of the tools—AWS CloudWatch, Nagios, and Splunk—is designed with distinct features to meet the varying needs of businesses. AWS CloudWatch forms a vital element of AWS by supplying statistics and logs for all the primary AWS services. They can use Metric Insights to adjust custom alarms, see data using dashboards, and easily pair with other AWS services, which fits well for big AWS users. Because it is deeply connected to AWS, resources can be easily scaled, and problems with operations can be spotted quickly. Therefore, AWS CloudWatch gives the most added value when an organization has built most of its services on AWS infrastructure, as there is greater emphasis on those tools than on non-AWS environments. Nagios, by contrast, is an acknowledged open-source product known for being flexible and working well on a wide range of systems. Monitoring of infrastructure as well as applications is done comprehensively, plus it comes with support for custom plugins that allow the monitoring of almost any device or system. The main benefit is its ability to adjust to customer needs, but people find it challenging to use or understand. Because it is open-source, using it saves businesses money when they can customize it, and they may find the interface works well for them, though some businesses may want a more modern design.

Splunk is designed to examine the data that IT systems produce. Because it indexes in real time and delivers first-rate analytics, it is ideal for businesses exploring both data types. Although Splunk is powerful in search, reporting, and visualization, it may be challenging for small companies or those with small budgets due to its complexity and price. Thanks to support for AWS and Azure, Splunk is a good fit for organizations using both public and private cloud services. The machine-driven analytics from Splunk add another layer of forecasting to the cloud infrastructure monitoring process. The selected monitoring system will depend on the infrastructure, the budget granted, and the organization's monitoring requirements. AWS CloudWatch is the preferred and most straightforward approach for any company that relies heavily on AWS. When organizations search for a single solution to oversee many systems simultaneously, Nagios may be the best option because of its flexibility and many plugins. Splunk is most appropriate for enterprises faced with complex data situations that rely on advanced analytics, searching, and visualization. A good approach is ensuring a tool suits a company's needs before building its cloud infrastructure. Cloud infrastructure monitoring is set to change as more artificial intelligence and machine learning are applied. Monitoring tools are expected to develop to act faster and automatically spot issues that might disrupt work. When AI insights are used, organizations can use their clouds more efficiently, reduce downtime, and safeguard resources. Due to the growing complexity of cloud infrastructure, there will be an increasing reliance on advanced, real-time monitoring tools like AWS CloudWatch, Nagios, and Splunk for performance, security, and cost management.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.

- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Aceto, G., Botta, A., De Donato, W., & Pescapè, A. (2013). Cloud monitoring: A survey. Computer Networks, 57(9), 2093-2115.

[2] Al Said, T. (2016). Enhancing security in public IaaS cloud systems through VM monitoring: a consumer's perspective (Doctoral dissertation, Cardiff University).

[3] Barth, W. (2008). Nagios: System and network monitoring. No Starch Press.

[4] Chavan, A. (2021). Exploring event-driven architecture in microservices: Patterns, pitfalls, and best practices. International Journal of Software and Research Analysis. https://ijsra.net/content/exploring-event-driven-architecture-microservices-patterns-pitfalls-and-best-practices

[5] Chavan, A. (2024). Fault-tolerant event-driven systems: Techniques and best practices. Journal of Engineering and Applied Sciences Technology, 6, E167. http://doi.org/10.47363/JEAST/2024(6)E167

[6] Dhanagari, M. R. (2024). MongoDB and data consistency: Bridging the gap between performance and reliability. Journal of Computer Science and Technology Studies, 6(2), 183-198. https://doi.org/10.32996/jcsts.2024.6.2.21

[7] Dhanagari, M. R. (2024). Scaling with MongoDB: Solutions for handling big data in real-time. Journal of Computer Science and Technology Studies, 6(5), 246-264. https://doi.org/10.32996/jcsts.2024.6.5.20

[8] Farshchi, M., Schneider, J. G., Weber, I., & Grundy, J. (2018). Metric selection and anomaly detection for cloud operations using log and metric correlation analysis. Journal of Systems and Software, 137, 531-549.

[9] Galletta, D. F., Henry, R., McCoy, S., & Polak, P. (2004). Web site delays: How tolerant are users?. Journal of the Association for Information Systems, 5(1), 1-28.

[10] Garland, K. J., & Noyes, J. M. (2004). Computer experience: a poor predictor of computer attitudes. Computers in Human Behavior, 20(6), 823-840.

[11] Grossi, G., Reichard, C., Thomasson, A., & Vakkuri, J. (2017). Theme: performance measurement of hybrid organizations–emerging issues and future research perspectives. Public Money and Management, 37(6), 379-386.

[12] Josephsen, D. (2007). Building a monitoring infrastructure with Nagios. Prentice Hall PTR.

[13] Konneru, N. M. K. (2021). Integrating security into CI/CD pipelines: A DevSecOps approach with SAST, DAST, and SCA tools. International Journal of Science and Research Archive. https://ijsra.net/content/role-notification-scheduling-improving-patient

[14] Lee, J. B., Yoo, T. H., Lee, E. H., Hwang, B. H., Ahn, S. W., & Cho, C. H. (2021). High-performance software load balancer for cloud-native architecture. IEEE Access, 9, 123704-123716.

[15] Lingamallu, P. K., & Oliveira, F. (2023). AWS Observability Handbook: Monitor, trace, and alert your cloud applications with AWS'myriad observability tools. Packt Publishing Ltd.

[16] Liu, C. H., & Chen, W. H. (2019). The study of using big data analysis to detecting APT attack. Journal of Computers, 30(1), 206-222. Barker, R. (2020). The uses and benefits of Splunk in continuous integration.

[17] Méndez Roca, M. (2020). New Innovations in eIDAS-compliant Trust Services: Anomaly detection on log data (Master's thesis, Universitat Politecnica de Catalunya).

[18] Mongkolluksamee, S., Pongpaibool, P., & Issariyapat, C. (2010, May). Strengths and limitations of Nagios as a network monitoring solution. In Proceedings of the 7th International Joint Conference on Computer Science and Software Engineering (JCSSE 2010). Bangkok, Thailand (pp. 96-101).

[19] Nikkhouy, E. (2016). Monitoring Service Chains in the Cloud.

[20] Parikh, A. (2019). Cloud security and platform thinking: an analysis of Cisco Umbrella, a cloud-delivered enterprise security (Doctoral dissertation, Massachusetts Institute of Technology).

[21] Poornalinga, K. S., & Rajkumar, P. (2016). Continuous integration, deployment and delivery automation in AWS cloud infrastructure. Int. Res. J. Eng. Technol.

[22] Pourmajidi, W., Steinbacher, J., Erwin, T., & Miranskyy, A. (2018). On challenges of cloud monitoring. arXiv preprint arXiv:1806.05914.

[23] Raj, P., Raman, A., Nagaraj, D., Duggirala, S., Raj, P., Raman, A., ... & Duggirala, S. (2015). Real-Time Analytics Using High-Performance Computing. High-Performance Big-Data Analytics: Computing Systems and Approaches, 161-185.

[24] Sandhu, R. S., & Samarati, P. (1997). Authentication, Access Controls, and Intrusion Detection. The Computer Science and Engineering Handbook, 1, 929-1.

[25] Sardana, J. (2022). Scalable systems for healthcare communication: A design perspective. International

Journal of Science and Research Archive. https://doi.org/10.30574/ijsra.2022.7.2.0253

[26] Sardana, J. (2022). The role of notification scheduling in improving patient outcomes. International Journal of Science and Research Archive. https://ijsra.net/content/role-notification-scheduling-improving-patient

[27] Singh, V. (2022). Visual question answering using transformer architectures: Applying transformer models to improve performance in VQA tasks. Journal of Artificial Intelligence and Cognitive Computing, 1(E228). https://doi.org/10.47363/JAICC/2022(1)E228

[28] Singh, V. (2023). Enhancing object detection with self-supervised learning: Improving object detection algorithms using unlabeled data through self-supervised techniques. International Journal of Advanced Engineering and Technology. https://romanpub.com/resources/Vol%205%20%2C%20No%201%20-%2023.pdf

[29] Solis Patrón, C. Y. (2015). Data Analytics as a Service: A look inside the PANACEA project (Master's thesis, Universitat Politècnica de Catalunya).

[30] Sommer, P. (1999). Intrusion detection systems as evidence. Computer Networks, 31(23-24), 2477-2487.

[31] Stephen, A., Benedict, S., & Kumar, R. A. (2019). Monitoring IaaS using various cloud monitors. Cluster Computing, 22(Suppl 5), 12459-12471.

[32] Verginadis, Y. (2023, March). A review of monitoring probes for cloud computing continuum. In International Conference on Advanced Information Networking and Applications (pp. 631-643). Cham: Springer International Publishing.

[33] Ward, J. S., & Barker, A. (2014). Observing the clouds: a survey and taxonomy of cloud monitoring. Journal of Cloud Computing, 3, 1-30.

[34] Weinman, J. (2012). Cloudonomics: The business value of cloud computing. John Wiley & Sons.

[35] Zadrozny, P., & Kodali, R. (2013). Big data analytics using Splunk: Deriving operational intelligence from social media, machine data, existing data warehouses, and other real-time streaming sources. Apress.