Comparison of Splunk and Nagios Devops Monitoring Tools and Their Use Cases

Carina Wickström, Ifeoma Urama

April 24, 2021

Abstract

Comparing products, especially in a Devops monitoring tools environment where there is a vast availability of tools to choose from, can sometimes be a daunting task. Companies are always looking to have best tool within their limited available resources. That is why this work is focused on comparing two popular DevOps monitoring tools; Splunk (proprietary Devops monitoring tool) and Nagios (free and open-source Devops monitoring tool). By comparing their features and uses cases, one can more easily pick the best option when deciding on which product to choose. From our studies we see that each of the products have their strengths and weakness. Both are good depending on what the user intend to achieve. So, it was found out that instead of these products competing with each other, they rather compliment each other. In conclusion, instead of using just one of them, we suggest using both, if the resources are available.

1 Introduction

Continuous monitoring is an essential part in the chain of processes required to implement a DevOps culture in the software development life cycle. Continuous monitoring starts once the application is deployed to the production server. Since the emergence of DevOps, companies and organizations have developed and adopted many different monitoring tools to support and improve this practice. The choice between such tools must be made in accordance with what they aim to achieve. Some tools are best suited for monitoring machine generated data, while others are more suitable for monitoring the health of the entire IT infrastructure to detect performance issues before they propagate to the user. Due to the amount of monitoring tools available, it can be difficult for companies to choose among them. Hence, it is of relevance to make a comparison of their features to facilitate the decision of which tool to select for a specific application.

This report aims to compare Nagios and Splunk, which are two of many popular tools for continuous monitoring. It will further discuss why continuous monitoring is important in a DevOps practice, and why companies and organizations are adopting this practice. The structure of this work is as follows: In section 2, we present the background of Nagios and Splunk. Section 3 provides a comparison of both monitoring tools, in terms of use cases, cost, and ease to use. Finally, in section 4, a conclusion of the comparison of both tools is presented.

2 Background

The need for faster development, regular testing and frequent release of software has brought forth the DevOps monitoring culture. It focuses on increasing awareness at every stage of the delivery pipeline [1], with continuous monitoring of planning, development, testing and integration, deployment and operations being an integral part of the development process.

2.1 Monitoring Tools

Monitoring tools are useful for not only software companies, but also for any company using IT infrastructure to get an overview of their system's behaviour. By using a monitoring tool, different aspects of a system can be surveyed, including the performance of servers, networks, databases, etc. By keeping track of the performance of such software units, system faults can be detected early on by finding the root cause. Even during any type of development, it is important to get feedback to enable developers to make changes when necessary. Additionally, system monitoring can serve as a preemptive measure for finding irregularities or symptoms that could, if untreated, lead to system faults. It is also important in maintaining and improving health and quality of IT systems' infrastructure. [2]

There are many alternative monitoring tools suitable for a DevOps workflow. The abundance of these options can make it difficult for companies to choose which monitoring tool to use. In addition, many websites on the internet that have ranked such monitoring tools differently [3, 4, 5]. Other than Splunk and Nagios, there exist other popular monitoring tools on the market, for example SolarWinds and Amazon Cloudwatch. Today, many companies provide monitoring tools differing in features, pricing, and ease to use. Further, different tools might focus on different types of monitoring. A few different monitoring features are [6]:

- Availability Monitoring - Monitors system availability, such as up-time to ensures system availability.
- Resource Monitoring - Watches resources consumption by system units such as CPU, memory and hard drive to ensure performance.
- Error Monitoring - Checks defects such as network errors, dropped packages, etc.

- Log Monitoring - Searches log file to find rules to detect important events.
- Security Monitoring - Collects and analyse information to detect unauthorized or suspicious behaviour in the system.
- Integration Monitoring - Ensures the different system parts can properly talk to each other.
- Process Monitoring - Stores logs and metrics of the entire process to ensure no issue is registered.

2.2 Splunk monitoring tool

Splunk is a closed source big machine data software analytic tool, used to monitor, search, visualize, and act on a set of data points in real time. The machine data is generated from sensors, devices, web applications, among others. Splunk is mostly used by big organisations that need a very reliable system to monitor a lot of their services. Splunk can be used to analyze structured, unstructured and semi-structured data from multiple sources and transform the data into a rich data representation depending on the context [7]. Splunk has four product categories namely [8]:

- Data to everything - provides real-time understanding of systems productivity, security, profitability and competitiveness. It comprises of splunk enterprise, splunk cloud and splunk data stream processor.
- Splunk for IT operations - Prevents disruptions in managing full stack service. This comprises of splunk infrastructure monitoring, Splunk IT service Intelligence, Splunk On-call
- Splunk for Security - Provides security operations with advance analytics to protect the system against latest threats. It comprises of splunk security essentials, splunk enterprise security, splunk phantom, splunk mission control, splunk user behaviour analytic, Splunk threat research.
- Observability - Use for problem detection. It comprises of Splunk infrastructure monitoring, Splunk Application performance monitoring and Splunk On-call.

Some of the advantages and disadvantages of using Splunk are [9]:

Advantages

- Real-time performance monitoring tool
- Faster trouble shooting result
- Machine learning capabilities
- Requires less hardware resources
- Real-time alert for desired search
- Provides breakdown of CPU/memory use
- Provides an enhanced GUI
- Accepts data in multiple format
- Analyses structured and unstructured data

Disadvantages

- Expensive
- Steep learning curve

2.3 Some of the Splunk use cases

Splunk has provided an all-inclusive solution for many uses cases such as security and IT operations. Some of its notable uses cases in area of security are; [10] cloud security, security monitoring, threat hunting, security operation center, management and collaboration, advanced threat detection, and audit and compliance.

2.4 Nagios monitoring tool

Nagios is a free and open source monitoring tool used for continuous monitoring of the entire IT infrastructure to ensure systems, services, applications and business

processes are functioning properly in a DevOps culture [11]. It is known to be an industry standard in an IT infrastructure [12]. Nagios uses plugins as standalone extensions to the core to periodically determine the current status of the hosts and services on the network. There are about 50 official Nagios plugins and over 3000 third party plugins available [13]. It is built on a server/agent architecture. On a network, Nagios' servers run on a host and the plugins interact with local and remote hosts that need to be monitored.

There are five Nagios product lines that deliver excellent solutions to several organisations worldwide[13]. They are;

- Nagios core - Is the industry standard and has been the de facto standard for infrastructure monitoring over decades.
- Nagios XI - Is the Nagios most powerful IT infrastructure alerting solution and provides unparalleled usability, flexibility and customized users needs.
- Nagios fusion - Is Nagios solution for operational status visualization to help resolve problems faster across an organization's entire IT infrastructure.
- Nagios log server - Is an enterprise-class log monitoring, management and analysis application for quick and easy view, analyses and query of logs from machine generated log data.
- Nagios network analyser - Is the commercial-grade network flow data analysis solution that provides network traffic and bandwidth information for the entire IT infrastructure.

Some of the advantages and disadvantages of using Nagios are [14]:

Advantages

- Free
- Open-source
- Extensive plugins available
- Customizable to users specific need
- Substantial user control

Disadvantages

- Requires many configuration
- Lacks user-friendly GUI
- No inherent notification settings
- Minimal customer support

2.5 Some of the Nagios use cases

Nagios offers some use cases to system administrators and managers [15]. To system administrators, the Nagios reactor provides automatic and mass software deployment, and auto-scale cloud computing when integrated with cloud solutions like AWS. For Managers, the event chain helps them streamline workflow and Return of Investment (ROI). Nagios can also be configured for task reminders and notification engines. Nagios XI provides planning capability, info of network health and activity [16].

3 Comparison

The choice between Splunk and Nagios could be a considerable factor when deciding which of these monitoring tool to work with. They are compared in terms of use cases, cost, and ease of use:

- Use case - Splunk has an advantage in terms of data log analysis. It is considered the best monitoring tool for capturing and analysing machine data. It provides logs of the whole system, which helps companies track down reasons for system downtime. Nagios on the other hand is better used for continuous monitoring. With a more advanced alert functionality, Nagios can better alert when for instance a server is down. Hence, Nagios can be used when the user is interested in tracking a specific metric, for example CPU, disk, memory, uptime, ping, etc. In conclusion, Nagios is better used for all-around availability monitoring compared to Splunk, which specializes in log analysis. Nagios will

answer the question "Is the service up?", while Splunk will answer "Why did the service go down?".

- Cost - In terms of cost, Nagios can be used for free, while Splunk can not. Splunk's licensing model depend on how much data is logged over a 24 hour period, which makes Splunk increasingly expensive for monitoring big amounts of data.
- Ease of use - In terms of ease of use, Nagios does not promise production support or as much documentation as Splunk provides. Nagios requires more coding effort, which increases with navigating among its large amount of third party libraries, as well as lack of documentation. Splunk is thereby easier to use thanks to its production support and documentation.

4 Conclusion

From our comparison we could see that both Nagios and Splunk have benefits and drawbacks. Splunk is a strong tool for monitoring events and log files. It is additionally easier to use due to documentation and less coding is required. However, it is expensive for system monitoring. In that regard, Nagios would be advantageous. Another advantage of Nagios is its many plugins and addons. So, the next question might be, can splunk and Nagios be used together?

Considering cost, we think it will be a good option to use both tools, since Splunk is proprietary and expensive for certain usage, where Nagios is free and open source. We can see that they rather compliment each other than compete with each other. Splunk is good at detecting errors and checking system health from log files. It provides especially good log retention, log reporting and event correlation. Therefore, Splunk is good when you don't know what to look for. So, use Splunk for monitoring events and log files and Nagios for system statistics and trending.

References

[1] Atlassian, "Devops monitoring." https://www.atlassian.com/devops/devops-tools/devops-monitoring. [Online, Accessed: 14 April 2021].

[2] Swicktech, "Why do my computer systems need monitoring?." https://www.swicktech.com/SWICKtech/Resources/Blog/Why-do-my-computer-systems-need-monitoring.htm. [Online, Accessed: 12 April 2021].

[3] Software Testing Help, "Top 10 popular server monitoring tools." https://www.softwaretestinghelp.com/top-10-popular-server-monitoring-tools/. [Online, Accessed: 14 April 2021].

[4] PC Network Downloads, "11 best network monitoring tools software of 2021." https://www.pcwdld.com/best-network-monitoring-tools-and-software. [Online, Accessed: 14 April 2021].

[5] ChannelE2E, "Top 10 most popular monitoring tools." https://www.channele2e.com/software/apps/10-most-popular-monitoring-tools-cloud-apm-web-and-more/. [Online, Accessed: 14 April 2021].

[6] DZone, "The different types of server monitoring software." https://dzone.com/articles/the-different-types-of-server-monitoring-software. [Online, Accessed: 12 April 2021].

[7] Splunk data stream processor, "product capabilities." https://www.splunk.com/en_us/software/stream-processing.html. [Online, Accessed: 15 April 2021].

[8] Splunk, "Splunk products." https://www.splunk.com/en_us/software.html. [Online, Accessed: 24 April 2021].

[9] tothenew, "Advantages of splunk and why to use it." https://www.tothenew.com/blog/why-should-you-use-splunk-for-log-analysis/. [Online, Accessed: 19 April 2021].

[10] Splunk, "Use cases." https://www.splunk.com/en_us/cyber-security.html. [Online, Accessed: 24 April 2021].

[11] Saurabh, "Nagios tutorial – continuous monitoring with nagios." https://www.edureka.co/blog/nagios-tutorial/. [Online, Accessed: 15 April 2021].

[12] nagiosvideo, "What is nagios?." https://www.nagios.com/products/. [Online, Accessed: 16 April 2021].

[13] Nagios, "Nagios plugins." https://www.nagios.org/projects/nagios-plugins/. [Online, Accessed: 16 April 2021].

[14] sites, "Itcs465-nagios - pros and cons." https://sites.google.com/site/itcs465nagios/protocols-supported. [Online, Accessed: 19 April 2021].

[15] Nagios, "Nagios reactor use cases." https://www.nagios.com/products/nagios-reactor/use-cases/. [Online, Accessed: 24 April 2021].

[16] Nagios, "Nagios xi use cases." https://www.nagios.com/products/nagios-xi/use-cases/. [Online, Accessed: 24 April 2021].