الـجـمـــهـوريـة الـجـزائـريـة الـديـمـقـراطـيـة الـشـعـبـيــة

People's Democratic Republic of Algeria

وزارة الـتـعـلـيـم الـعـالـي والـبـحـث الـعـلـمــي

Ministry of Higher Education and Scientific Research

المــــدرســـة الـوطـنـيـة العليا للـتـكـنـولـوجـيـات المـتـقـدمـة

Ecole Nationale Supérieure des Technologies Avancées

GÉNIE ELECTRIQUE ET INFORMATIQUE INDUSTRIEL

Report Project to Obtain the Diploma of

Master

- Field -

Telecommunication

- Specialty -

Telecommunication Systems and Networking

- Subject -

Comparison of Different Monitoring and Alerting Tools in IT Infrastructure

Realized by

Aya Alia Abdi & Rima Boubeghel

Members of the Jury :

Mr Tarek Cherifi	Chair
Mr Abdelkader Balahcene	Examiner
Mme Lila Abbad	Examiner
Mr El Hadi Khoumeri	Supervisor

Algiers, Jun 25th 2024

Academic year 2023-2024

Comparison of Different Monitoring and Alerting Tools in IT Infrastructure

Aya Alia Abdi*, Rima Boubeghel†, El Hadi Khoumeri‡
*†‡*Electrical Engineering and Industrial Computing*
National Higher School of Advanced Technology
Algiers, Algeria
*y_abdi@ensta.edu.dz, †r_boubeghel@ensta.edu.dz, ‡elhadi.khoumeri@ensta.edu.dz

***Abstract*—Monitoring is crucial for all companies as it enables systematic observation and analysis of various aspects of IT infrastructure using specialized tools. These tools provide capabilities for visualization, alerting, and anomaly prediction, along with additional features unique to each tool. This paper compares eight of the top monitoring tools of 2024, offering an overview of their functionalities and key considerations for selecting the most suitable option for a company's needs.**

***Index Terms*—Monitoring, Alerting, IT infrastructure, Nagios XI, Zabbix, LibreNMS, Prometheus, Grafana, Dynatrace, New Relic, Datadog**

I. Introduction

In today's digital world, where computers and IoT devices are everywhere, a reliable monitoring tool is crucial for businesses to keep an eye on all the activities at the same time. A monitoring tool can be defined as software designed to simultaneously observe various activities, gather data, analyze it, generate reports, and issue notifications and alerts to administrators as needed. The monitoring system tracks the performance, network usage and storage of IT infrastructure, including physical devices, virtual machines, applications, services and container-based environments.

An effective monitoring system uses visuals and alerts to keep you informed. These visual representations provide a high-level view of the IT environment, while alerts notify IT staff of issues such as service outages so they can be quickly resolved. Moreover, by analyzing historical data and trends, the system can even predict potential problems and prevent them from occurring.

There are many monitoring solutions available, from free open-source options to paid licenses, Choosing the right monitoring tool depends on several parameters including the alerting system, functionality, flexibility, scalability, deployment, maintenance, integration with the existing system, and cost. The cost consideration not only includes the software license cost but also encompasses expenses associated with staff training and support.

The objective of this paper is to provide an overview of some of the best IT infrastructure monitoring tools available in 2024, alongside a detailed comparison based on various factors that should be considered when selecting the right tool for your architecture.

The rest of the paper is structured as follows: Section II outlines the factors to consider when selecting the appropriate monitoring tool. In Section III, we provide a comparison of the most widely recognized monitoring tools available in the market. Finally, the paper concludes with the last Section, offering a summary of the findings and a look to the future.

II. Methodology

Before delving into the various monitoring tools available in the market, it is crucial to thoroughly assess the entire IT infrastructure. For instance, it is necessary to determine whether there is a traditional setup involving servers and network equipment, or if the environment incorporates newer technologies such as cloud services and containers. Identifying the specific resources that need to be monitored beforehand is essential. Additionally, consider the type of data to gather from these resources. Metrics alone might not be sufficient; other data such as traces, events, and logs could also be critical depending on the needs. Moreover, the scale of the company should also influence the choice of a monitoring tool. Whether a small business or a large enterprise, scalability is an important factor to consider, as it will ensure the tool can accommodate growth and changes in the infrastructure. Also, consider factors such as the capabilities of the IT department and the programming languages used in the infrastructure to ensure compatibility with the monitoring tool. It is important that the chosen tool can integrate smoothly with the existing systems and that the team is equipped to utilize it effectively [1],[30].

After creating a comprehensive report on the entire stack, it's time to choose the right monitoring tool to ensure effective monitoring. The monitoring tool should meet specific criteria. Below, the most important parameters to consider when selecting a monitoring tool are introduced, aiming to find the perfect match for the needs.

A. Data collection

Understanding the different methods used to collect data from the targets is important. This includes an agent-based approach, which involves installing software on monitored systems, an agentless approach, which utilizes built-in monitoring technologies and protocols such as WMI –Windows Management Instrumentation– and SNMP –Simple Network

Management Protocol– , a hybrid approach combining both agent and agentless approach [3].

B. Alerting Mechanism

Alerting is one of the most critical features of monitoring tools. These tools trigger alerts based on predefined conditions such as threshold breaches, anomalies, or specific events. The configuration of these alerts depends on the tool being used, and they are then delivered to various notification channels like email, PagerDuty, etc., to notify users or system administrators.

C. Data Visualization

This key feature involves the ability to transform complex data into meaningful representations that are easily comprehensible to your IT department team, enabling them to quickly identify issues, facilitate troubleshooting, recognize patterns, spot anomalies, and more.

D. Scalability

A monitoring system that functions effectively for a small architecture may not necessarily perform well for larger architectures. Therefore, scalable monitoring solutions are designed to adapt and accommodate growth and change while ensuring reliability and performance. For example, the monitoring system can manage changes in the number of targets by utilizing features like service discovery and automatic discovery to minimize manual configurations [2].

E. Integration

This feature offers the flexibility to integrate diverse services like Kebernetes with monitoring tools, enhancing specific functionalities as required.

F. Ease of use

This parameter encompasses the entire deployment process, from installation to maintenance [3]. Consider the complexity of working with the monitoring tool and evaluate its user interface: does it provide a user-friendly UI to facilitate interaction?

G. Cost

Cost is always an important consideration. With a thorough understanding of how the tool will impact your organization, calculate the total cost of ownership [1].

These are the main factors to consider while choosing your IT infrastructure monitoring tool.

III. COMPARATIVE ANALYSIS

In this section, we'll explore some of the most widely used infrastructure monitoring tools available, examining their features. It's important to note that while every monitoring and alerting tool shares a similar global architecture, they differ in the functionalities and services they provide. Figure 1 illustrates the global architecture of an infrastructure monitoring tool. The monitoring approach varies based on the method used to collect data, such as employing agents or exporters among others.

Here is a comparative analysis of selected tools

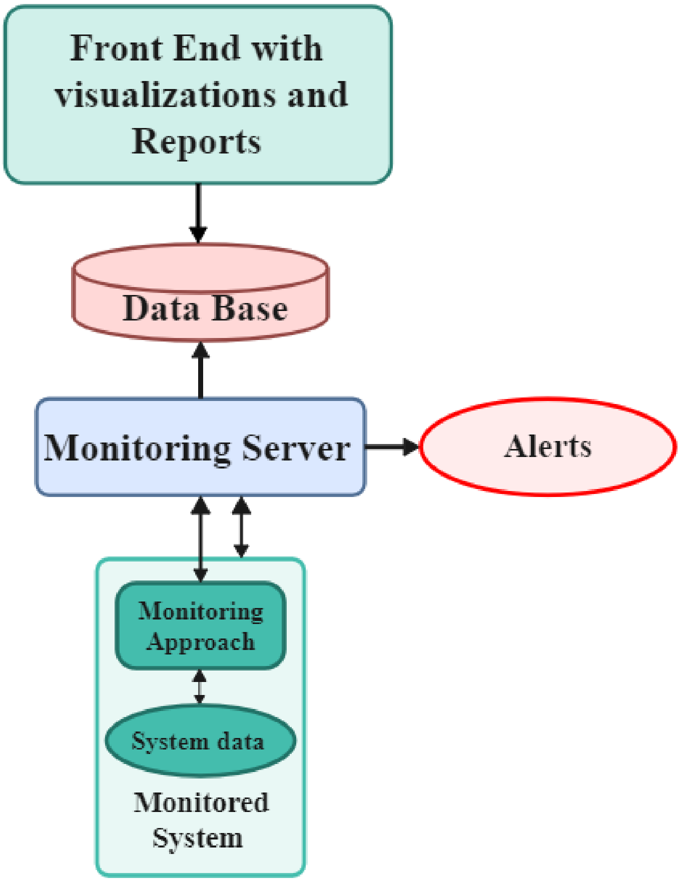

Fig. 1. Infrastructure monitoring tool architecture

A. Nagios XI

Nagios is one of the oldest real time tools for monitoring IT infrastructure. It was launched in 1999 as NetSaint by Ethan Galstad. It is licensed under GNU GPL –General Public License– V2. Nagios has a free open-source version Nagios Core and a paid version Nagios XI. Many features are missing on Nagios Core [4]. Nagios XI collects metrics from various targets such as servers, end-user stations, network equipment, and other services using both agent-based and agentless configurations. On one hand, Nagios XI supports a wide range of agents for many operating systems, including long-running options such as NRPE, NSCA, and NSClient++. NCPA (Nagios Cross Platform Agent) is a newer option that can be used on any machine running Linux, Windows, OSX, AIX, and Solaris 1. On the other hand, Nagios XI benefits from different protocols like SNMP and SSH for agentless monitoring [6].

Nagios XI excels at network monitoring, as it can track almost any network device. It supports the monitoring of common protocols such as HTTP, FTP, SNMP, SMTP, POP3, and ICMP among others. Moreover, it uses plugins to extend its networking capabilities which makes it eligible to monitor any service or protocol [26].

Nagios XI can be combined with Nagios Network Analyzer, Log Server, and Nagios Fusion to develop an IT management system that is custom designed for your specific environment.

Nagios XI features an updated web interface that provides a high-level overview of monitored resources and an easy-to-use interface to enhance performance [1],[5],[18].

B. ZAbbix

Zabbix, an enterprise-level open source monitoring tool, was first introduced in 2001. It is both flexible and feature-rich, offering a setup process that is comparatively easier than those of other monitoring tools [7].

The major components of Zabbix include the Zabbix server, agent, database, and web interface. These components enable users to efficiently collect metrics from their IT infrastructure, including network equipment, servers, virtual machines, and cloud services. Agents are installed on target devices to gather metrics for the Zabbix server. These agents perform both passive and active checks: passive checks occur when the agent responds to data requests from the Zabbix server, while active checks require the agent to first retrieve a list of items from the Zabbix server for independent processing and then periodically transmit updated values back to the server. In situations where agent installation is not feasible or the target does not permit remote installations, Zabbix also supports agentless monitoring using protocols and techniques like SNMP, IPMI, JMX, SSH, and Telnet [7], [8].

One of the main reasons Zabbix is easy to use is its simple web interface. This interface simplifies the setup process for anyone, requiring minimal time to learn due to its template design for items, triggers, and graphs [9], [10].

C. LibreNMS

LibreNMS, an open-source monitoring tool founded in 2013, offers a wide range of beneficial features for monitoring operating systems and networks. LibreNMS supports agents for data collection from systems. Additionally, it is compatible with multiple protocols such as SNMP, OSPF, and ARP, enabling the retrieval of metrics from devices that do not support agent installation [7].

The LibreNMS Web UI allows users to conveniently add monitored devices, similar to the process in Zabbix. Among the supported features of LibreNMS are auto-discovery, an application programming interface (API), auto-updating, and more [7], [11].

D. Prometheus

Prometheus is an open-source monitoring and alerting toolkit that enjoys robust support from a highly active community of developers and users. Developed in 2012 at SoundCloud, It has been incubated by the Cloud Native Computing Foundation since 2016 [25], [31].

The toolkit, written in Go, is licensed under the Apache 2.0 license. Prometheus was originally designed to facilitate near-real-time monitoring of dynamic, cloud- and container-based microservices, services, and applications. However, it has also become widely adopted for monitoring traditional architectures. It collects metric data through a pull mechanism from various targets such as servers, databases, applications, and web servers via HTTP endpoints. The collected time series data are stored locally, but Prometheus also supports remote storage, enabling the transfer of data from the server to alternate storage solutions [25].

Users can query and aggregate data using Prometheus's own query language PromQL, which allows for the creation of new time series from existing data and the establishment of rules to save frequently used queries and aggregations [25].

Prometheus includes a dedicated component, Alertmanager, where users can define and manage alerts, which can be sent through multiple channels including email and PagerDuty.

Featuring high scalability and performance, Prometheus excels even in large network environments. It supports service discovery through various methods such as static configurations, file-based discovery, and automated discovery, efficiently managing monitored resources.

Prometheus can be integrated with third-party tools like Grafana to create sophisticated and customized visualizations.

E. Grafana

Grafana is an open-source software developed by Torkel Ödegaard in 2014. It is a time-series data querying tool with a query editor, a visualization platform featuring dashboards, and an alerting system [12], [13].

Grafana is one of the most fascinating data visualization technologies, offering significant expansion in capabilities and scope due to its excellent visualization compared to other visualization tools as shown Figure 2. It features the capability to visualize data in the form of graphs, histograms, or heatmaps utilizing axes, lines, points, fills, annotations, and more [14].

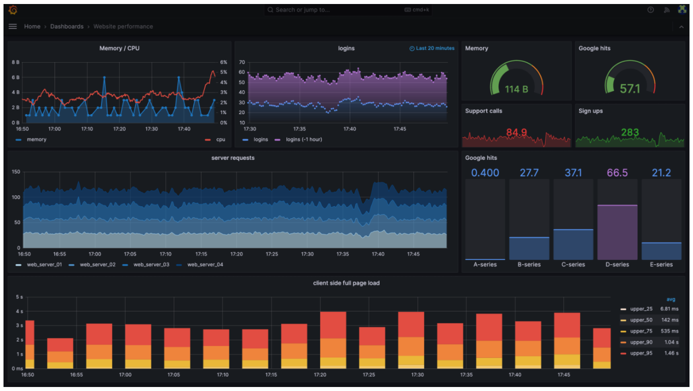

Fig. 2. Grafana visualization

It has a data source model which is highly pluggable and supports multiple time-series-based data sources like Prometheus, InfluxDB, and Graphite. Additionally, it has the capacity to support combining data from different sources into a single dashboard [12].

F. Dynatrace

Dynatrace is a paid software intelligence platform founded in 2005, specifically developed to assist organizations in effectively monitoring, managing, and optimizing the performance of their systems. By providing real-time insights and advanced observability features, Dynatrace ensures comprehensive monitoring across all components of your infrastructure. It offers full automation throughout the deployment, instrumentation, discovery, dependency mapping, problem identification, and root cause analysis processes [15], [16].

To utilize this tool, you only need to install OneAgent on the host, which collects data from diverse sources such as the containers, virtual machines, networks, servers, storage, and more. This makes Dynatrace a flexible tool for monitoring the entire system [16].

Dynatrace features Dynatrace Real User Monitoring (RUM), a component that gathers all data pertaining to a user's interaction with an application. This includes metrics such as request start time, navigation start time. The application can be a web application, mobile application, or custom application. Additionally, RUM can easily identify any errors or problems that arise [17]. Additionally, Dynatrace is characterized by the use of artificial intelligence, especially for predicting future values and detecting anomalies.

G. New Relic

New Relic was founded in 2008 by Lew Cirne. Interestingly, the company's name is an anagram of the founder's name, ”Lew Cirne.” For the third consecutive year, New Relic has been recognized as a Leader and an Outperformer in the 2024 GigaOm Radar for Cloud Observability [24].

New Relic is a full-stack monitoring tool uniquely offering a unified data platform that integrates all telemetry data—including events, metrics, logs, and traces—to provide complete visibility across your entire infrastructure [29].

New Relic offers more than 470 integrations including Kubernetes, Docker, Serverless, as well as AWS, Azure, and GCP services.

This performance monitoring tool offers a range of valuable features. It includes application performance monitoring (APM), which tracks real-time metrics such as error rates and response times. Synthetic monitoring allows you to simulate user interactions with your application to ensure optimal performance. Additionally, the tool provides robust error tracking and infrastructure monitoring, among other features.[29].

H. DataDog

Dadatog is the world's leading monitoring solution for cloud-scale applications, used to monitor servers, databases, tools and services to offer a unified perspective of the entire infrastructure. This functionality is accessible through a SaaS-based data analytics platform. The company was established in 2010 by Olivier Pomel and Alexis Le-Quoc. Datadog has earned notable recognition, it was listed in Forbes' Cloud 100 and was ranked among the top ten fastest growing companies in North America in Deloitte's 2016 Fast 500 List [19].

Datadog offers a wide array of features that support the latest technologies. Figure 3 provides an illustration of Datadog's functionalities, including its diverse features and services [23].

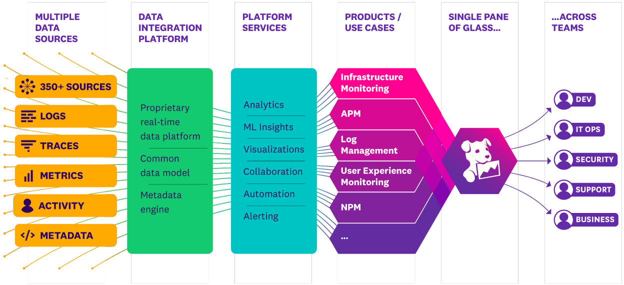

Fig. 3. Architectual overview of datadog monitoring tool features and services

Datadog collects data through open-source Datadog agents installed on target machines. These agents transmit metrics and host events automatically to the Datadog platform, where you can evaluate and analyze the data effectively.

With Datadog, you can also monitor and identify cyber threats throughout your applications, network, and infrastructure.Additionally, datadog offers a mobile app that enables you to receive and view alerts directly on your mobile device [20].

Datadog features an advanced alerting system that leverages machine learning to detect anomalies, identify issues, and trigger alerts. It automatically applies these alerts to new targets, ensuring that you can scale your environment without missing anything. Additionally, you can easily direct notifications to communication platforms such as Slack, Hangouts Chat, and Microsoft Teams [21].

Datadog offers more than 700 built-in integration, enabling it to pull data from almost every service you use. It features robust cloud integration capabilities, allowing you to unify views across multiple clouds such as Azure and AWS and on-premises infrastructures [27, 28]. This integration enhances your visibility and allows for extensive customization of your dashboards. Additionally, Datadog provides predictable pricing, based on monitored entities and features used [22].

The comparative analysis of infrastructure monitoring tools reveals distinct features and functionalities across various platforms. Nagios XI, Zabbix, LibreNMS, Prometheus, Grafana, Dynatrace, New Relic, and Datadog all share a common architecture but differ in their approach to data collection and monitoring. Nagios XI excels in network monitoring with extensive agent support, while Zabbix offers a simpler setup and versatile agentless monitoring options. Prometheus is noted for its robust support in dynamic environments and integrates seamlessly with Grafana for advanced visualizations. Dynatrace and New Relic provide comprehensive full-stack monitoring with AI-driven insights, whereas Datadog stands out with its extensive integrations and advanced alerting system. Each tool caters to specific needs, making the choice dependent on the specific requirements of the infrastructure.

The following TABLE I presents the main characteristics of each tool, including License, Data Collection methods, Data Type, Alerting capabilities, Visualization options, Deployment Location, Integration capabilities, Auto-discovery features, and other notable Features. This table aims to provide a clear and concise overview to aid in the selection of the most appropriate monitoring tool for specific needs.

The comparative analysis highlights distinct features and functionalities among the infrastructure monitoring tools discussed. Each tool offers unique approaches to data collection, alerting, visualization, and integration. The summary table provides a clear overview of the key characteristics, aiding in the selection process based on specific requirements. Whether prioritizing network monitoring, advanced visualization, understanding the strengths and limitations of each tool is crucial for effective infrastructure monitoring.

IV. CONCLUSION

In conclusion, this article has provided a comprehensive overview and comparison of eight of the most widely used IT infrastructure monitoring tools in 2024, including Prometheus, Grafana, and Datadog. By examining their features and similarities, we have highlighted the unique strengths each tool offers. Key parameters such as scalability, ease of integration, cost, and user interface have been discussed to guide companies in selecting the right tool for their specific needs.

As we look to the future, it is clear that monitoring tools must evolve to support emerging trends such as cloud integration, the incorporation of machine learning (ML) and artificial intelligence (AI) capabilities. These advancements will enable more sophisticated predictive analytics and automated responses, enhancing the ability to manage and optimize IT infrastructure proactively. Adapting to these trends will be essential for companies seeking to maintain a robust and efficient IT environment in the rapidly changing technological landscape.

TABLE I
EIGHT POPULAR IT INFRASTRUCTURE MONITORING TOOLS

Tool	**Nagios XI**	**Zabbix**	**LibreNMS**	**Prometheus**	**Grafana**	**Dynatrace**	**New Relic**	**DataDog**
License	paid	Open Source	Open Source	Open Source	Open Source	Paid	Paid	Paid
Data collection	-Agent-based -Agentless	-Agent-based -Agentless	-Agent-based -Agentless	-Exporters	Relies on data sources to collect data	-Agent-based, known as OneAgent -Agentless	-Agent-based -Agentless	-Agent-based -Agentless
Data type	-Metrics	-Metrics -Logs -Events	-Metrics -Logs	-Metrics	-Metrics -Logs -Traces	-Metrics -Logs -Events -Traces	-Metrics -Logs -Events -Traces	-Logs -Traces -Metrics
Alerting	Supports alerting mechanism	Supports alerting mechanism	Supports alerting mechanism	Supports alerting mechanism	Supports alerting mechanism	Flexible alerting system using ML	Flexible alerting system using ML	Advanced alerting system using ML
Visualization	Excellent	Good	Basic	Basic	Excellent	Excellent	Excellent	Excellent
Deployment Location	Cloud/ On-premises, OS supported: RHEL CentOS Ubuntu Debian	Cloud/ On-premises, OS supported: RHEL CentOS Ubuntu Debian Oracle Linux	Cloud/ On-premises, OS supported: RHEL CentOS Ubuntu Debian Ubunto Gentoo	Cloud/ On-premises	Cloud/ On-premises	Cloud (SaaS)	Cloud(SaaS)/ On-premises	Cloud (SaaS)
Integration	-Integration with: Cloud platforms -Virtualization platforms -Database systems -IT service management (ITSM) -Ticketing systems And multiple plugins	-Integration with: ticketing/helpdesk systems -Configuration management systems -Messaging systems -Visualization/ Reporting systems -Inventory management systems	-Alerting Systems -Ticketing Systems -Visualization Tools	-Service Discovery integrations like Kuma -Remote storage integrations like AWS -Timestream Etc	+290 built-in integration	+620 built-in integration	+470 built-in integration	+700 built-in integration
Auto discovery	Yes	Yes	Yes	Yes	Not concerned with it	Yes	Yes	Yes
Features	-Wide Community -support Multiple plugins -Network Monitoring	-Offers high scalability and flexibility c -Multiple plugins	-Ease of use and installation -Ease of configuration -Flexible -Auto-updating	-Active community of developers and users High performance	-Public dashboards Visualisations -suggestions Infinity datasource plugin	-Intelligent observability -Application Security powerful automation -Offers Dynatrace mobile app	-Synthetic monitoring -Application performance monitoring (APM) -Error tracking	-Wide range of integrations -Supports multiple cloud platforms and DevOps teams collaboration -Offers mobile app

References

[1] Hernantes, J., Gallardo, G., & Serrano, N. (2015). IT infrastructure-monitoring tools. IEEE software, 32(4), 88-93.

[2] Sarkar, I. (2023). Scalable automated monitoring solution for virtual infrastructure.

[3] Kufel, Ł. (2016). Tools for distributed systems monitoring. Foundations of computing and decision sciences, 41(4), 237-260.

[4] Chahal, D., Kharb, L., & Choudhary, D. (2019). Performance analytics of network monitoring tools. Int. J. Innov. Technol. Explor. Eng. IJITEE, 8(8).

[5] https://assets.nagios.com/handouts/nagiosxi/Nagios-XI-Features.pdf.

[6] Gandikota, V. R., & Sowjanya, A. M. REMOTE PROCESS AUTOMATION OF MONITORING USING NAGIOS.

[7] Leppänen, T. (2021). Data visualization and monitoring with Grafana and Prometheus.

[8] Olups, R. (2016). Zabbix Network Monitoring. Packt Publishing Ltd.

[9] Lahti, C. B., & Peterson, R. (2007). Sarbanes-Oxley IT compliance using open source tools. Elsevier.

[10] https://woshub.com/zabbix-install-configure-guide/

[11] https://docs.librenms.org/General/Updating/

[12] https://grafana.com/docs/grafana/latest/introduction/

[13] Chakraborty, M., & Kundan, A. P. (2021). Grafana. In Monitoring cloud-native applications: Lead agile operations confidently using open source software (pp. 187-240). Berkeley, CA: Apress.

[14] Abbasi, M. B. (2021). Observability of Industrial Data using an Analytics and Monitoring Platform (Master's thesis).

[15] https://sematext.com/glossary/dynatrace/

[16] Ahola, J. (2022). Cloud monitoring: cloud monitoring with dynatrace.

[17] https://docs.dynatrace.com/docs/platform-modules/digital-experience/rum-concepts/rum-overview

[18] https://assets.nagios.com/downloads/nagiosxi/docs/Using-Auto-Discovery-In-Nagios-XI.pdf

[19] https://www.datadoghq.com/about/latest-news/press-releases/deloitte-2016-fast-500/

[20] https://www.devopsschool.com/blog/top-50-datadog-interview-questions-and-answers/

[21] https://www.datadoghq.com/product/platform/alerts/

[22] https://docs.datadoghq.com/integrations/

[23] https://cloudiogram.com/total-visibility

[24] https://newrelic.com/sites/default/files/2023-06/Company_Fact_Sheet_2023.pdf

[25] Turnbull, J. (2018). Monitoring with Prometheus. Turnbull Press.

[26] bin Mohd Shuhaimi, M. A. A., binti Roslan, I., & binti Anawar, S. (2011, December). The new services in Nagios: Network bandwidth utility, email notification and sms alert in improving the network performance. In 2011 7th International Conference on Information Assurance and Security (IAS) (pp. 86-91). IEEE.

[27] Brinkmann, A., Fiehe, C., Litvina, A., Lück, I., Nagel, L., Narayanan, K., ... & Thronicke, W. (2013, December). Scalable monitoring system for clouds. In 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing (pp. 351-356). IEEE.

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

[29] Nalla, K. R., & El-Ocla, H. (2016). Response Time Analysis of Mobile Application DNUN in New Relic Monitoring Platform.

[30] Boccia, V., Carraciuolo, L., Del Prete, D., Pardi, S., Antonacci, M., Donvito, G., ... & Bellotti, R. (2014, September). Infrastructure Monitoring for distributed Tier1: The ReCaS project use-case. In 2014 International Conference on Intelligent Networking and Collaborative Systems (pp. 557-562). IEEE.

[31] Pivotto, J., & Brazil, B. (2023). Prometheus: Up & Running. " O'Reilly Media, Inc.".