St. Francis Institute of Technology, Mumbai-400 103
Department Of Information Technology

A.Y. 2023-2024
Class: TE-ITA/B, Semester: V

Subject: **Advanced DevOps Lab**

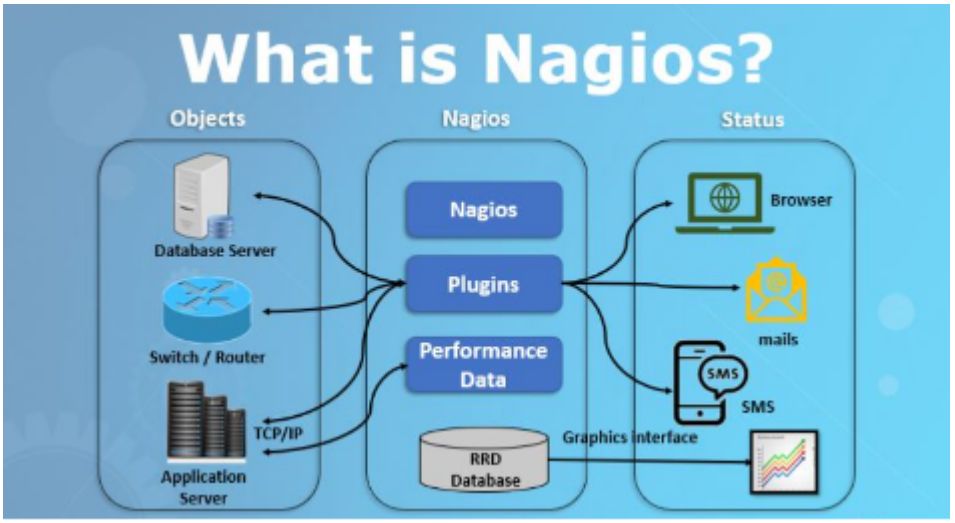
Experiment –9: To explain continuous monitoring and installation and configuration of Nagios Core, Nagios Plugins and NRPE (Nagios Remote Plugin Executor) on AWS EC2 linux machine.

1. **Aim:** To explain continuous monitoring and installation and configuration of Nagios Core, Nagios Plugins and NRPE (Nagios Remote Plugin Executor).
2. **Objectives:** Aim of this experiment is that, the students will learn:
   - How to launch a new pre-installed Nagios XI server in the Amazon EC2 cloud in order to quickly run a trial of Nagios XI without using physical hardware, migrate existing physical installations to a cloud infrastructure, and/or scale an existing XI monitoring environment.
3. **Lab objective mapped : ITL504.5:** To use Continuous Monitoring Tools to resolve any system errors (low memory, unreachable server etc.) before they have any negative impact on the business productivity
4. **Prerequisite:**
   - NIL
5. **Requirements:** AWS account, browser, Personal Computer, Windows operating system, Internet Connection, AWS CLI
6. **Pre-Experiment Exercise:**

Brief Theory :

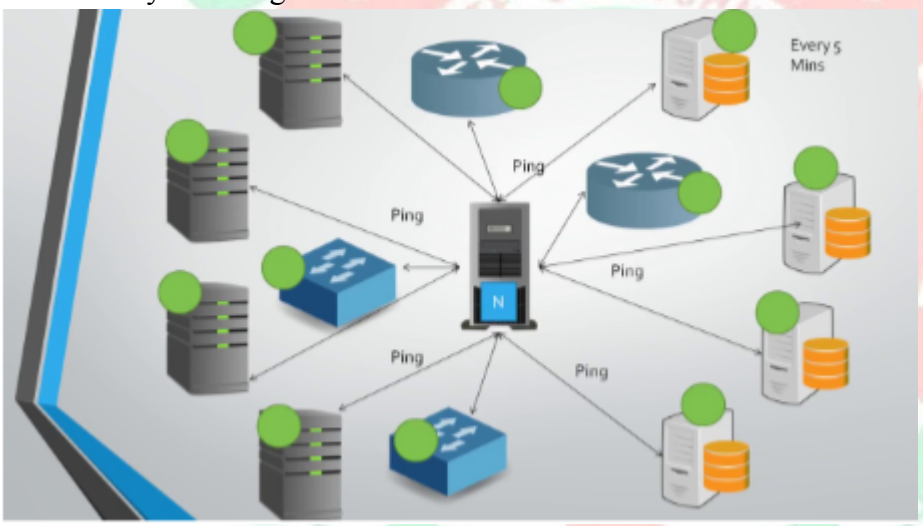
Introduction Nagios:

Nagios is an open-source monitoring tool that provides comprehensive monitoring and alerting capabilities for IT infrastructure. It is designed to help system administrators and IT professionals monitor their IT infrastructure's health, performance, and availability, including servers, switches, routers, and other network devices. It helps organizations proactively identify and resolve issues, ensuring smooth operations and minimizing downtime. In this case study, we will explore how a company implemented Nagios to enhance its IT infrastructure monitoring and alerting system, resulting in improved efficiency, reduced downtime, and enhanced overall performance.



Why to use Nagios?

The main aim of Nagios is continuous monitoring of IT infrastructure. Nagios is designed to provide real-time, 24/7 monitoring of various aspects of an organization IT environment, including servers, networks, applications, and services. Its primary goal is to ensure the availability, reliability, and performance of these systems by continuously checking their status and health.



Why do we need Continuous Monitoring?

Continuous monitoring is vital in the world of IT to swiftly detect and resolve issues, both technical and security-related. It provides real-time insights into system health, enabling proactive problem-solving and minimizing downtime. This ongoing vigilance is essential for ensuring optimal performance, reducing risks, and maintaining the reliability and security of computer systems and networks.

Why Nagios is used for Continuous Monitoring?

Nagios facilitates continuous monitoring by conducting automated and scheduled checks on various aspects of IT infrastructure, including servers, services, and network devices. It uses customizable plugins to perform these checks, evaluating the results against predefined thresholds. When issues or anomalies are detected, Nagios triggers

alerts through various communication channels. This continuous monitoring process ensures that system administrators receive real-time information about the health, performance, and availability of critical components. By proactively identifying and notifying about problems, Nagios assists in rapid issue resolution, reduces downtime, and supports efficient resource management in complex IT environments.

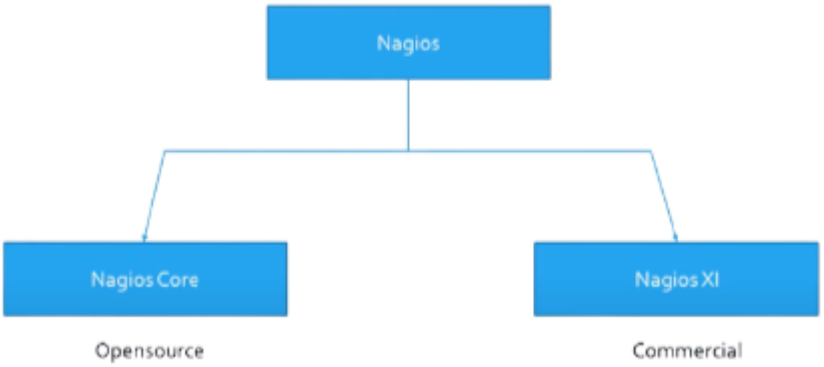
Advantages of using Nagios:
1. Centralized monitoring: Nagios provides a single, unified view of the entire IT infrastructure. This enables the IT team to monitor and manage all components from a centralized dashboard, improving efficiency and reducing the time spent on issue identification.
2. Downtime Mitigation: Nagios detects and alerts on system issues, such as server failures or service disruptions, minimizing unplanned downtime.
3. Proactive Problem Resolution: Continuous monitoring allows early detection of anomalies, enabling IT teams to proactively address problems, often before they impact users.
4. Resource Optimization: Nagios monitors resource utilization (CPU, memory, disk space) to optimize resource allocation, preventing resource exhaustion and bottlenecks.
5. Automated alerting and notifications: Nagios automates the alerting process, sending notifications to the IT team whenever an issue occurred. This minimizes response time and ensured timely resolution of critical issues, enhancing business continuity.
6. Security Enhancement: It identifies security threats and suspicious activities, enhancing network security by providing timely alerts for potential breaches.
7. Performance Optimization: Nagios monitors and reports on system performance, helping administrators fine-tune configurations and improve overall system efficiency.
8. Planned Maintenance: It supports planned maintenance windows, allowing for updates and maintenance without disrupting ongoing operations.
9. Data-Driven Decision-Making: Nagios collects performance data, enabling data analysis for informed decisions, capacity planning, and trend analysis.

Key Features of Nagios:
1. Continuous Monitoring: Nagios continuously checks the health and status of hosts, services, and network devices in real time.
2. Alerting and Notifications: It provides customizable alerting and notification mechanisms, ensuring that IT teams are promptly informed of issues via email, SMS, or other communication methods.
3. Threshold-Based Alerts: Nagios allows administrators to define thresholds for monitored metrics. When a metric exceeds or falls below these thresholds, it triggers alerts.
4. Resource Utilization Monitoring: Nagios monitors resource utilization, including CPU, memory, disk space, and network bandwidth, helping optimize resource allocation and detect performance bottlenecks.
5. Security Monitoring: Nagios can integrate with security tools and monitor logs and events for signs of security breaches, unauthorized access, or unusual activities.

6. Customizable Plugins: Nagios relies on plugins to perform specific checks. It supports a vast library of built-in plugins and allows for the creation of custom plugins to monitor unique aspects of the IT environment.
7. Performance Data Collection: Nagios collects performance data during monitoring checks, enabling administrators to analyse trends and make informed decisions about resource allocation and capacity planning.
8. Automation: It can be configured to execute automated actions or responses when specific conditions are met, such as restarting services or scaling resources.
9. Downtime Scheduling: Nagios supports planned downtime scheduling, preventing unnecessary alerts during maintenance windows.
10. Centralized Dashboard: It provides a centralized web-based dashboard where administrators can view the current status of all monitored components and access historical data and reporting tools.
11. Community and Ecosystem: Nagios has an active user community and a vast ecosystem of plugins, extensions, and integrations available to extend its functionality.
12. Scalability: Nagios can scale to monitor small to large and complex IT environments, accommodating the growth of organizations.
13. Open-Source: Nagios is an open-source tool, making it cost-effective and allowing for flexibility and customization.

Applications of Nagios:
1. Infrastructure Monitoring: Nagios keeps an eye on the health and performance of servers, network devices, and services to ensure smooth operations and proactively identify potential issues of an organization's infrastructure.
2. Application Monitoring: It ensures that critical applications, such as web servers, databases, and email servers, are always available and performing optimally. If issues arise, Nagios sends alerts for quick resolution.
3. Network Monitoring: Nagios extends its monitoring capabilities to network devices like switches, routers, and firewalls. It detects network outages, traffic spikes, and other network-related problems, helping ensure network reliability.
4. Log Monitoring: Nagios Log Server provides the ability to search, analyze, and set up alerts for log data generated by various systems and applications. This feature assists in troubleshooting and identifying issues by examining log information.
5. Service Monitoring: Nagios can monitor a wide range of services, including HTTP, FTP, DNS, SMTP, and more, verifying that these services are functioning correctly and accessible to users.
These are just a few examples of how Nagios can be applied in various IT environments. Its flexibility and wide range of monitoring capabilities make it a valuable tool for organizations to ensure the stability and reliability of their IT infrastructure.

Types of Nagios:



1. Nagios Core:
   Nagios Core is the foundational, open-source version of the Nagios monitoring platform. It serves as the heart of the Nagios ecosystem, providing essential monitoring and alerting capabilities. In Nagios Core, administrators manually define what to monitor and how by configuring text-based configuration files. While it offers a robust and highly customizable monitoring solution, it requires users to have a good understanding of the system's configuration and scripting. Nagios Core is supported by a vibrant user community that contributes to plugins and extensions, making it a popular choice for organizations seeking cost-effective, flexible, and tailored monitoring solutions.
2. Nagios XI:
   Nagios XI is the commercial counterpart to Nagios Core, designed toenhanceuser-friendliness and add advanced features. While building on the core functionality of Nagios Core, Nagios XI provides a user-friendly web interface for configuration, monitoring, and reporting. It offers features like auto-discovery, which simplifies device detection and monitoring setup, making it suitable for large and complex environments. Nagios XI also includes advanced reporting and graphing capabilities, improving data visualization and analysis. The commercial version is backed by Nagios Enterprises, offering commercial support, training, and consulting services, making it an ideal choice for organizations with extensive monitoring needs and a desire for enhanced usability and support.

Challenges Faced: Before implementing Nagios:
1. Lack of centralized monitoring: The organization had multiple monitoring tools in place, leading to fragmented monitoring. This made it difficult to get a holistic view of the entire infrastructure and identify potential issues.
2. Manual alerting process: The existing system relied on manual checks and notifications, leading to delays in identifying and resolving issues. This resulted in increased downtime and impacted business operations.
3. Inefficient resource allocation: The company struggled to allocate resources effectively due to the lack of real-time monitoring and visibility into the infrastructure. This led to overprovisioning or underutilization of resources, affecting cost optimization.

Implementation of Nagios:

To address these challenges, Nagios is implemented as the centralized monitoring and alerting solution. The implementation process involved the following steps:

1. Setup and Installation:

a. Choose the appropriate version of Nagios (Core or XI) based on your monitoring requirements and resources.

b. Install Nagios on a dedicated server or virtual machine. Follow the installation instructions for your chosen version and Linux distribution.

c. Configure Nagios by defining hosts, services, and checks in the configuration files. You can use text-based configuration files or a web interface, depending on the version you are using.

d. Set up notification options, such as email alerts or SMS notifications, to be informed of monitoring events.

2. Host and Service Configuration:

a. Define the hosts you want to monitor. This could include servers, network devices, and other infrastructure components.

b. Specify the services to monitor on each host. Services could be web servers, databases, email servers, etc.

c. Configure thresholds and parameters for each service check. For example, set CPU usage alerts to trigger when usage exceeds a certain percentage.

3. Testing and Validation:

a. Verify your Nagios configurations using the built-in tools and command-line utilities provided by Nagios. This ensures that your setup is error-free.

b. Test service checks to ensure they are working as expected. For example, manually trigger a check to see if it generates the correct alert.

4. Monitoring and Alerting:

a. Once your configurations are validated, Nagios will continuously monitor the defined hosts and services.

b. Nagios will generate alerts and notifications when it detects issues based on your defined thresholds and criteria. These alerts can be sent to administrators or teams responsible for resolving the issues.

5. Troubleshooting and Resolution:

a. When an alert is received, investigate the underlying issue. The Nagios interface provides details on what triggered the alert.

b. Resolve the issue based on the information provided. This may involve fixing a server problem, restarting a service, or taking other corrective actions.

6. Performance Analysis and Reporting:

a. Nagios collects performance data over time. Use this data to analyze trends, identify recurring issues, and make data-driven decisions for infrastructure improvements.

b. Generate reports and graphs to visualize performance and availability data. This helps in tracking the overall health of your infrastructure.

7. Ongoing Maintenance:

a. Regularly update Nagios and its plugins to ensure you have the latest features and security patches.

b. Adjust configurations as your infrastructure changes. Add new hosts and services as needed and remove those that are no longer in use.

c. Monitor and manage the Nagios system itself to ensure its health and availability.

8. Documentation and Training:

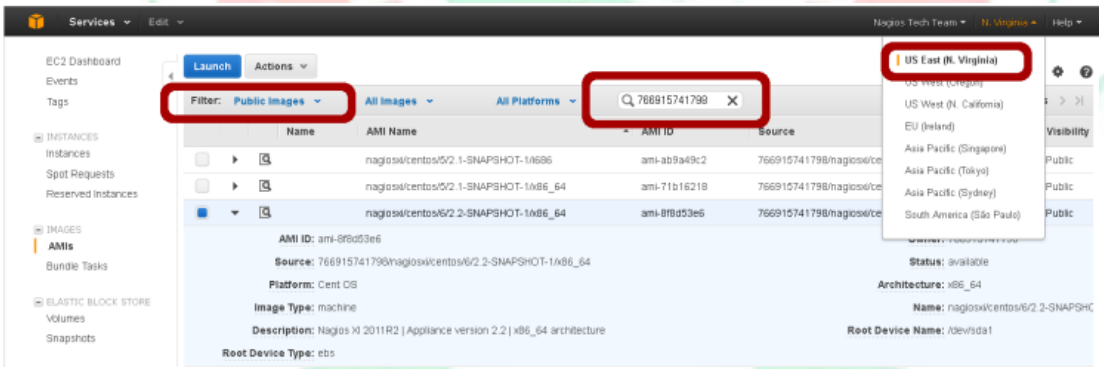
a. Maintain documentation of your Nagios setup, configurations, and procedures for troubleshooting and maintenance.

b. Provide training to your IT team on how to use Nagios effectively and interpret alerts and performance data.

7. Laboratory Exercise :

Steps to install and spin up a Kubernetes cluster on Linux machine/cloud platforms. (attach SS)

1: Creating The Virtual Machine



Images are currently available in the following zones:

- US East (N. Virginia & Ohio), US West (N. California & Oregon)
- Canada (Central)
- EU (Frankfurt, Ireland, London)
- Asia Pacific (Mumbai, Seoul, Singapore, Sydney, Tokyo)
- S. America (Sao Paulo)

Making sure you are using the appropriate region and have the filter set to: **Public Images.**

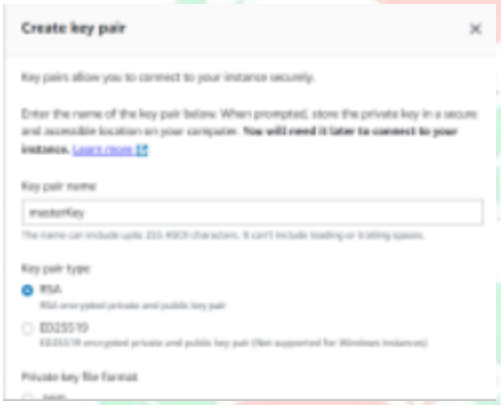
In the search bar enter: 766915741798. This is the Nagios Tech Team official ID. From here you can select the image that meets your needs and click Launch.

Next, the Request Instance Wizard will begin. Within the wizard you will be able to select your instance type and customize the allocated resource settings and naming information. For Nagios XI, the minimum specifications we recommend are 1 core and 2GB RAM.

The wizard will have you choose, or create a key pair. If you are creating a key pair for

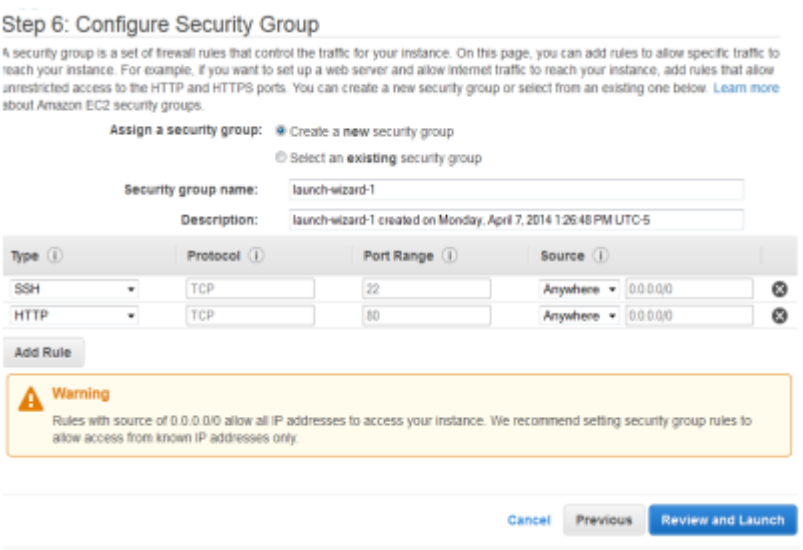
the first time, you will be asked to download the key before continuing. The private key will be required to SSH into your machine.

2. Create a new key pair



Note: root password login is disabled.

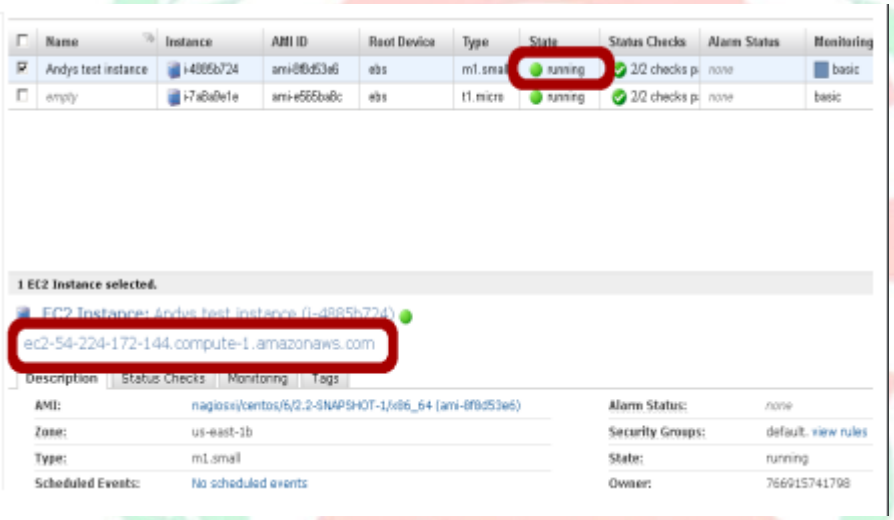
3. Additionally you will be asked to select or configure a Security Group. The Security Group should allow public access on port 22 and port 80, this may be fine for some installations, however keep in mind that you will also require the use of additional ports that you will be sending your network flow data to



Note: When you first start your instance, the latest version of Nagios XI is installed and compiled at boot. This will take at least 15 minutes before the instance will become available. The amount of time will depend on the instance size you create

4. Connecting To Nagios XI

Once the instance is running, you can complete the installation of Nagios XI through the web interface. To access Network XI, type in the following URL: http://<ipaddress>/nagiosxi (where <ipaddress> is the IP address of the virtual machine)



Note: You can find the Public DNS address by selecting the instance and viewing the details.

5. Once you access the login screen, you can log in as the Admin to begin using Nagios XI. The credentials are listed below.

XI Admin Account:

Username: nagiosadmin

Password: random (this gets initialized during setup)

MySQL Account:

Username: root

Password: nagiosxi

You may also need to occasionally make an SSH connection to your machine. This connection must use the private key you downloaded earlier. When connecting you must use the username ec2-user, NOT root, this user has full sudo access.

ssh -i .ssh/mykey.pem ec2-user@[AWS_public_DNS]

6. If you are having trouble with the configuration, make sure that your security group in Amazon EC2 includes information regarding Email. Outbound email may not work if the AMI doesn't have a valid DNS name, or your firewall rules don't allow outbound

SMTP except through a proxy.

8. **Post-Experiments Exercise**
   1. **Extended Theory:**(soft copy)
      1. What is the primary goal of Nagios in IT infrastructure monitoring?
      2. How does continuous monitoring benefit IT operations?
      3. What types of items can Nagios monitor within an IT environment?
      4. Name some key features of Nagios?
      5. Write challenges company faces before implementing Nagios?
   2. **Questions:**(write in hand)
      1. List and explain few applications of Nagios?
      2. What are the two main types of Nagios mentioned in the information?

   C. **Conclusion:**(write in hand)

   1. Write what was performed in the experiment
   2. Mention few applications of what was studied.
   3. Write the significance of the studied topic

   3. **References:**

      1. documentation: https://assets.nagios.com/downloads/nagiosxi/docs/Changing-Default-Passwords-in-Nagios-XI.pdf
      2. Forums: https://support.nagios.com/forum
      3. The Nagios Support Knowledgebase is also a great support resource: https://support.nagios.com/kb
      4. Nagios-https://www.nagios.org/
      5. Nagios - Network, Server and Log Monitoring Software-https://www.nagios.com/
      6. Use this Nagios monitoring tutorial for proactive IT monitoring-
      7. https://www.techtarget.com/searchitoperations/tutorial/Use-this-Nagios-monitoring-
      8. tutorial-for-proactive-IT-monitoring
      9. https://www.youtube.com/watch?app=desktop&v=2RKCr5P2FKA
      10. https://www.youtube.com/watch?v=s9xCXZNVpac
      11. https://en.wikipedia.org/wiki/Nagios
      12. https://www.educba.com/nagios-monitoring-tool/

——----------——----------