VIETNAM NATIONAL UNIVERSITY HOCHIMINH CITY

UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORKS AND COMMUNICATIONS



Midterm Report: Networks and Systems Administration

Project: Nagios

Lecturer: Trần Thị Dung

**Students:**

**Nguyễn Ngọc Trà My 21520353**

**Lê Hoàng Oanh 21521253**

**Bùi Hoàng Trúc Anh 21521817**

[I. Introduction 3](#_Toc154864195)

[**1.1** **General information** 3](#_Toc154864196)

[**1.2** **Component** 4](#_Toc154864197)

[**1.3** **Operation** 6](#_Toc154864198)

[II. Implementation 7](#_Toc154864199)

[**2.1** **Topology** 7](#_Toc154864200)

[**2.2** **Installation** 9](#_Toc154864201)

[**2.3** **Configuration** 12](#_Toc154864202)

[III. Results 18](#_Toc154864203)

[**3.1** **Monitor Windows** 19](#_Toc154864204)

[**3.2** **Monitor Linux** 19](#_Toc154864205)

[**3.3** **Monitor Web Server** 19](#_Toc154864206)

[IV. Demonstration 20](#_Toc154864207)

[V. Appendix 20](#_Toc154864208)

[**1.** **Self-evaluation** 20](#_Toc154864209)

[**2.** **Task Assignment** 20](#_Toc154864210)

[**3.** **Q&A** 20](#_Toc154864211)

1. **Introduction**
   1. **General information**

Nagios, an influential open-source monitoring system, empowers organizations to preemptively identify and rectify IT infrastructure issues before they impact essential business operations. Since its inception, it has undergone significant development and refinement. Let's delve deeper into the key aspects of Nagios.

* **History and Development:**

Originally released in 1999 as NetSaint, Nagios was developed by Ethan Galstad and subsequently refined by numerous contributors as an open-source project. Nagios Enterprises, a company based around the Nagios Core technology, offers multiple products, such as Nagios XI, Log Server, Network Analyzer and Fusion.

* **Versatile Platform:**

Nagios is designed to run primarily on the Linux operating system but boasts compatibility with a variety of platforms, including Linux, Windows, and Unix-based operating systems. This flexibility makes it an ideal choice for organizations with diverse IT environments.

* **Monitoring Capabilities:**

Nagios' monitoring capabilities extend across a broad spectrum of critical parameters, covering application, network, and server resources. It can vigilantly oversee memory usage, disk utilization, microprocessor load, the number of active processes, and log file statuses. Furthermore, Nagios excels in monitoring network services, including Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Hypertext Transfer Protocol (HTTP), and numerous other common network protocols.

* **Active and Passive Checks:**

Nagios employs both active and passive checks to evaluate the health and performance of monitored elements. Active checks are initiated by Nagios itself, while passive checks are received from external applications integrated with the monitoring system. This dual approach ensures comprehensive monitoring and real-time feedback.

* **Advanced Features:**

Nagios offers advanced features that set it apart. It supports the establishment of network host hierarchies, enabling a structured and efficient monitoring setup. Event handlers can be implemented to enable automated responses to detected issues, reducing the risk of service disruptions. Redundancy is a core feature, ensuring uninterrupted monitoring. Nagios also utilizes network topology analysis to determine dependencies, assisting in the swift identification of root causes when issues arise.

* **Scalability and User-Friendly Interfaces:**

Nagios is known for its scalability, adaptability, and security. It proactively safeguards the stability, performance, and security of systems, networks, and services. Informative and visually appealing web interfaces enhance the user experience and streamline access to vital monitoring data.

In summary, Nagios stands as a versatile and powerful monitoring tool, offering organizations a proactive approach to maintain the reliability of their IT infrastructure. Its adaptability, scalability, and extensive feature set, coupled with an active open-source community, make it an invaluable asset for businesses seeking robust IT infrastructure monitoring solutions.

* 1. **Component**

The architecture of Nagios is built on the basis of server-client architecture. The server of Nagios usually run on a host and the plugins run on the remote server/ or remote host which are to be monitored. The plugins of Nagios collect the useful data and send them to the process scheduler, which displays the information over the graphical user interface (GUI). Following are the three main components in the architecture of Nagios application:

* **Scheduler:**

The scheduler in Nagios, also known as one of the critical components within Nagios Core, orchestrates the monitoring process. It serves as the server component, performs checks on plugins at specified intervals according to configuration settings. This component takes actions according to the results gathered from the plugins. These actions might involve alerting the staff or automatically triggering scripts to resolve issues.

The scheduler is responsible for distributing monitoring tasks across the monitoring worker processes or threads. It can handle dependencies between services and hosts, ensuring that checks are performed in the correct order and that notifications are sent appropriately.

In addition to its core scheduling functions, Nagios can be extended using various add-ons, such as "Nagios Event Broker," which allows seamless integration with third-party tools, enhancing its capability for event processing and data manipulation.

* **Plugins:**

Nagios plugins provide low-level intelligence on how to monitor various aspects within the Nagios Core. These plugins operate as standalone applications, designed specifically to be executed by Nagios Core. They gather crucial data, enabling the system to assess and interpret the health and performance of monitored elements.

Nagios has a large community of plugins available, and custom plugins can also be created. They enhance Nagios' monitoring capabilities and allow for flexible and customized monitoring of various systems and applications.

For Windows machines, the Checknt plugin is commonly used for monitoring servers. To enable monitoring on a Windows computer, NSClient++ needs to be installed on that computer. NSClient++ acts as a client-side plugin that communicates with the monitoring server.

The communication between the server and the host is typically established using a secure socket layer (SSL) connection. This ensures that the information exchanged between the two parties is encrypted and secure.

To monitor Linux machines, the NRPE (Nagios Remote Plugin Executor) plugin is used. NRPE allows the monitoring server to execute plugins on the remote Linux machine and retrieve the monitoring data.

* **GUI:**

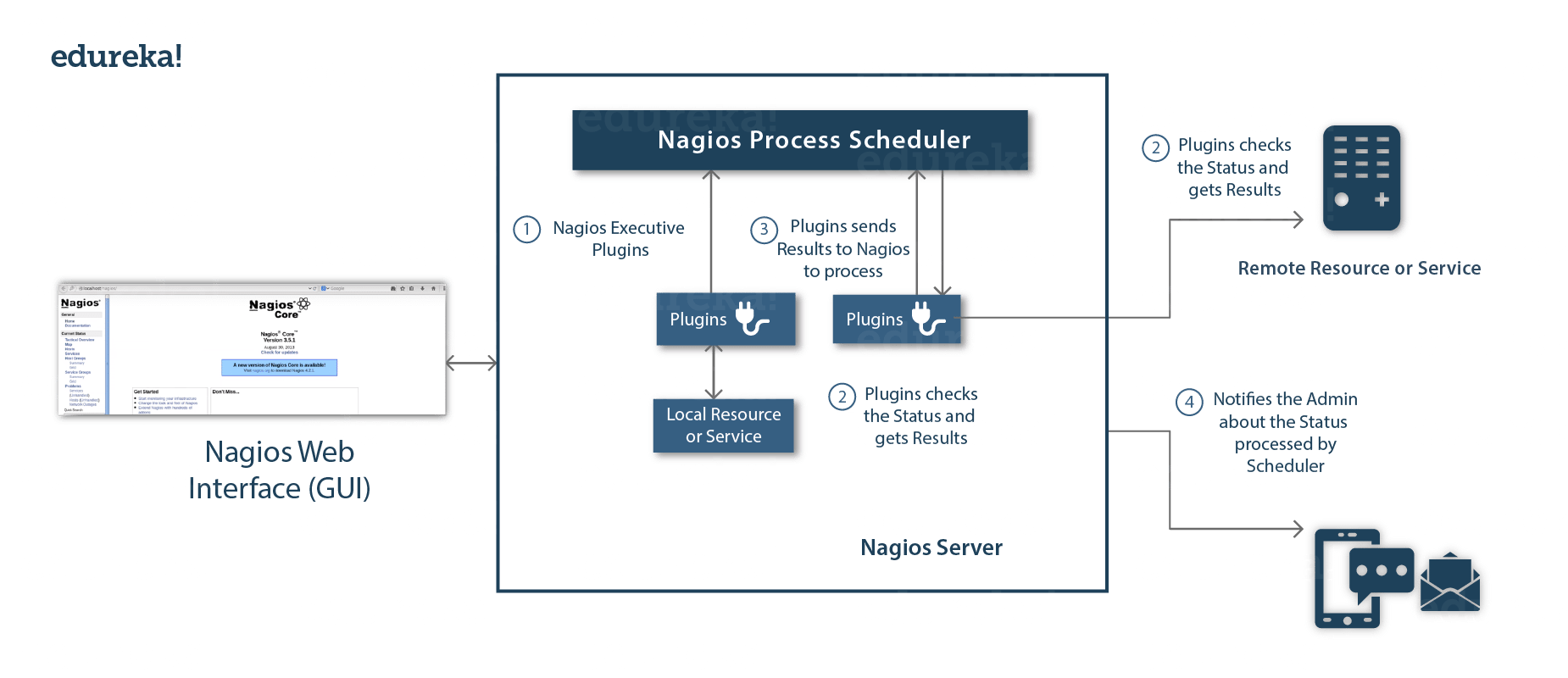
Nagios provides a web-based graphical user interface (GUI) to present the monitoring information in a user-friendly manner. This interface offers a visual representation of the monitored data, utilizing color codes, graphs, and sounds to denote the status of monitored elements. When a soft alert is triggered multiple times, it can escalate to a hard alert, prompting the Nagios server to send notifications to administrators or concerned personnel.

Additionally, the community and third-party developers have contributed significantly to the Nagios ecosystem by developing various frontends. These frontends, including Nagios Core, Nagios XI, and open-source alternatives like Icinga, Thruk, Checkmk, and Centreon, provide different levels of features and support to meet diverse monitoring needs.

* 1. **Operation**

Nagios is capable of monitoring hosts and services in two ways: actively and passively.

* Active checks are initiated by Nagios process and then run on a regular scheduled basis. The check logic inside Nagios process starts the Active check. To monitor hosts and services running on remote machines, Nagios executes plugins and tells what information to collect. Plugin then gets executed on the remote machine where is collects the required information and sends then back to Nagios daemon. Depending on the status received from hosts and services, appropriate action is taken. These are executed on regular intervals, as defined by check\_interval and retry\_interval.
* Passive checks are performed by external processes and the results are given back to Nagios for processing. An external application checks the status on hosts/services and writes the result to External Command File. When Nagios daemon reads external command file, it reads and sends all the passive checks in the queue to process them later. When these checks are processed, notifications or alerts are sent depending on the information in check result. Thus, the difference between active and passive check is that active checks are run by Nagios and passive checks are run by external applications. These checks are useful when hosts/services cannot be monitored on a regular basis.

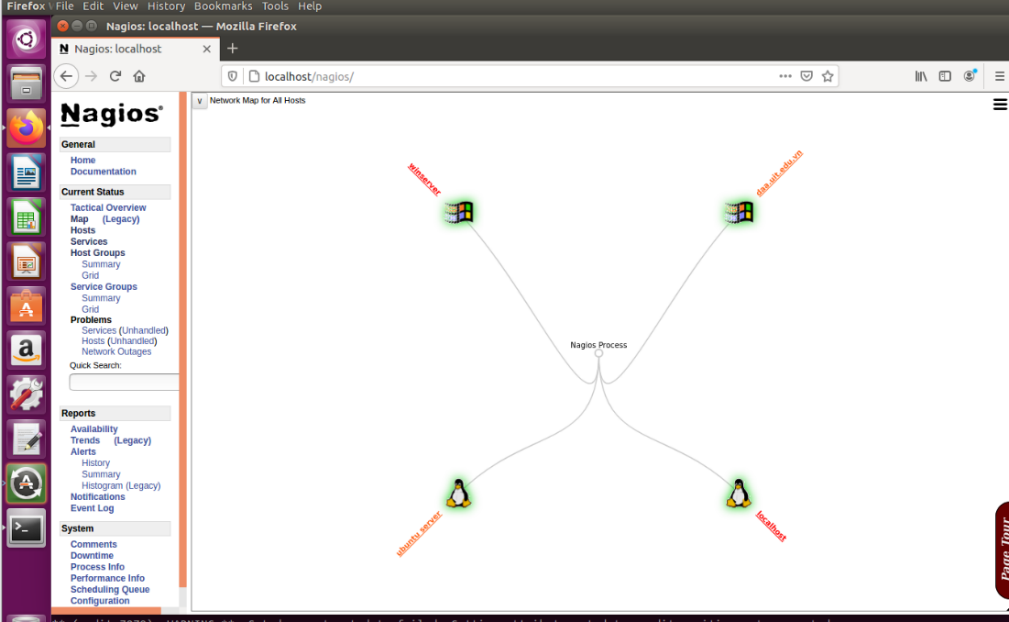


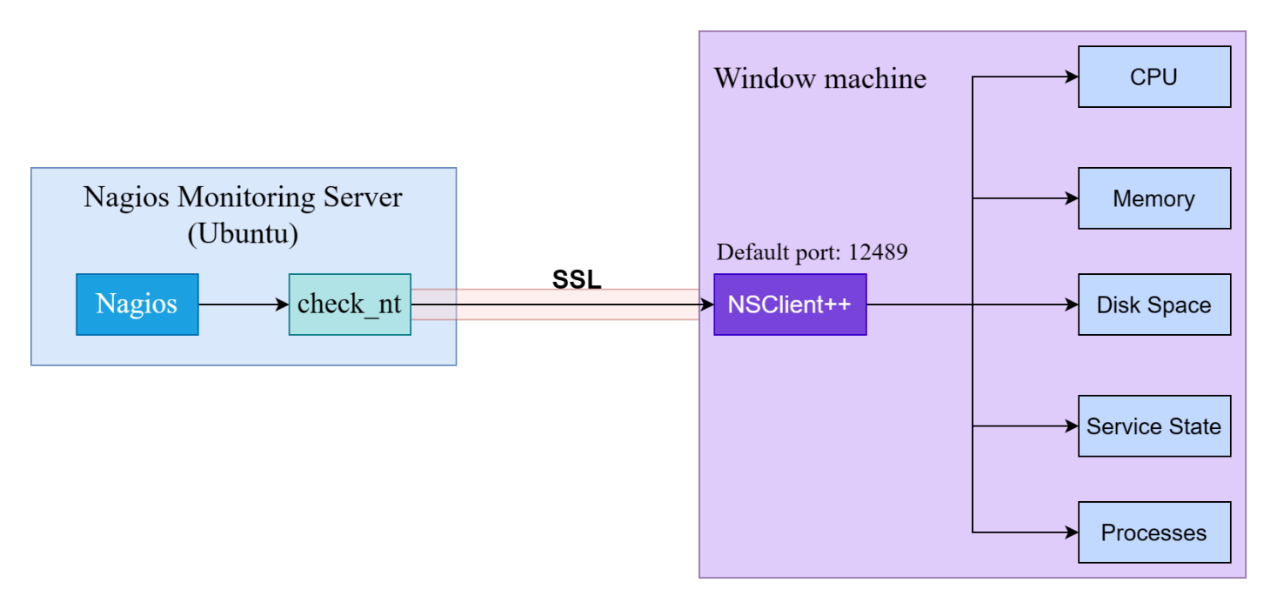
We focus on active checks when using Nagios to monitor hosts or services. The operation of the active checks in Nagios will be explained in detail. Nagios is a client-server architecture. Usually, on a network, a Nagios server is running on a host, and plugins are running on all the remote hosts which should be monitored.

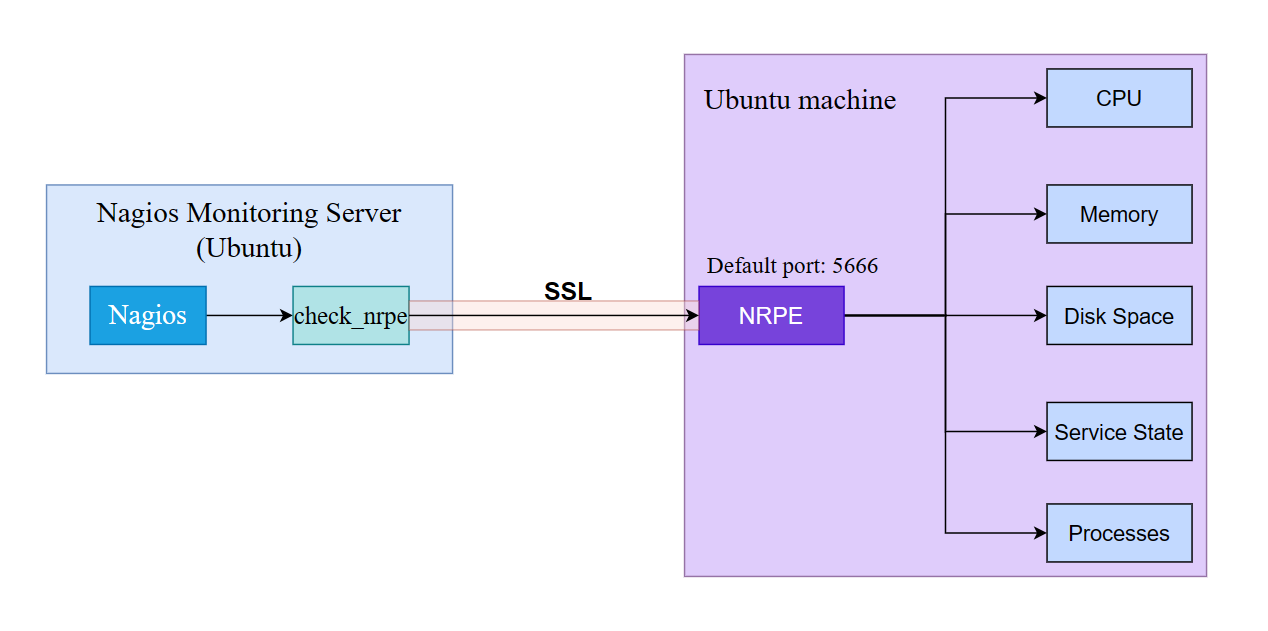
1. Scheduler sends signals to execute plugins on these remote hosts at the specified intervals. These plugins are tasked with gathering crucial status information from the target systems.
2. The Plugin, executed at the remote host, acts as the bridge between the Nagios server and the remote hosts. It runs the actual checks, collects data, and sends the acquired status information back to the Nagios server. This communication typically occurs over a network connection established between the remote host and the Nagios server.
3. Once the Plugin has collected the status information, it forwards this data to the Process Scheduler running on the Nagios server. The scheduler processes and updates the current state of the monitored resources, such as hosts or services, based on the received information.
4. As the process scheduler updates the internal state, it also ensures that the Nagios Graphical User Interface (GUI) reflects the latest monitoring status. Simultaneously, the process scheduler triggers notifications to be sent to designated administrators or support teams, informing them about the current state of the monitored resources. Notifications can be delivered through various channels, including email, SMS, or other communication methods, depending on the configured notification settings. By continually updating the GUI and sending notifications, Nagios enables administrators to promptly identify and respond to potential issues.

In summary, Nagios' architecture and operation are designed to provide comprehensive monitoring and alerting capabilities for networked systems. The Scheduler initiates checks, Plugins gather status data, the Process Scheduler centralizes and processes this data, the GUI provides a user-friendly interface, and timely notifications keep administrators informed and enable them to take swift corrective actions. This orchestration of components ensures that Nagios remains an invaluable tool for maintaining the stability and reliability of complex IT environments.

1. **Implementation**
   1. **Topology**







Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, Hình chữ nhật

Description automatically generated

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Ip Address | Default Gateway | Installation |
| Nagios Monitoring Server  (Ubuntu 16.04.7) | 192.168.12.137 | 192.168.12.1 | Nagios Core |
| Windows Client (Windows server 2019) | 192.168.1.2 | 192.168.1.1 | NSClient++ |
| Linux Client  (Ubuntu 16.04.7) | 192.168.12.135 | 192.168.12.1 | NRPE |

* 1. **Installation**
* **Set up Ubuntu 16.04.7 (Nagios monitoring server): Nagios Core**

**Step 1**: Run the following command to install pre-required packages:

*sudo apt-get install wget build-essential apache2 php apache2-mod-php7.0 php-gd libgd-dev sendmail unzip libkrb5-dev libssl-dev*

**Step 2**: Next, create user and group for Nagios and add them to Apache www-data user.

*sudo useradd nagios*

*sudo groupadd nagcmd*

*sudo usermod -a -G nagcmd nagios*

*sudo usermod -a -G nagios,nagcmd www-data*

**Step 3**: Download the latest Nagios package.

*wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.3.tar.gz*

**Step 4**: Extract the tarball file.

*tar -xzf nagios-4.4.3.tar.gz*

*cd nagios-4.4.3/*

**Step 5**: Run the following command to compile Nagios from source.

*./configure --with-nagios-group=nagios --with-command-group=nagcmd*

**Step 6**: Run the following command to build Nagios files.

*make all*

**Step 7**: Run the command shown below to install all the Nagios files.

*sudo make install*

**Step 8**: Run the following commands to install init and external command configuration files.

*sudo make install-commandmode*

*sudo make install-init*

*sudo make install-config*

*sudo /usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-available/nagios.conf*

**Step 9**: Now copy the event handler directory to Nagios directory.

*sudo cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/*

*sudo chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers*

**Step 10**: Download and extract Nagios plugins.

*wget https://nagios-plugins.org/download/nagiosplugins-2.2.1.tar.gz*

*tar -xzf nagios-plugins\*.tar.gz*

*cd nagios-plugins-2.2.1/*

**Step 11**: Install Nagios plugins using the below command.

*./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl*

*make*

*sudo make install*

**Step 12**: Now edit the Nagios configuration file.

*sudo gedit /usr/local/nagios/etc/nagios.cfg*

Uncomment line number 51: cfg\_dir=/usr/local/nagios/etc/servers

**Step 13**: Now, create a server directory.

*sudo mkdir -p /usr/local/nagios/etc/servers*

**Step 14**: Edit contacts configuration file. (change the email to the user’s email address)

*sudo gedit /usr/local/nagios/etc/objects/contacts.cfg*

**Step 15**: Now enable the Apache modules and configure a user nagiosadmin.

*sudo a2enmod rewrite*

*sudo a2enmod cgi*

*sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin*

*sudo ln -s /etc/apache2/sites-available/nagios.conf /etc/apache2/sites-enabled/*

**Step 16**: Now, restart Apache and Nagios.

*service apache2 restart*

*service nagios start*

*cd /etc/init.d/*

*sudo cp /etc/init.d/skeleton /etc/init.d/Nagios*

**Step 17**: Edit the Nagios file.

*sudo gedit /etc/init.d/Nagios*

Adding the following text to the Nagios file:

DESC = "Nagios"

NAME = nagios

DAEMON = /usr/local/nagios/bin/$NAME

DAEMON\_ARGS = "-d /usr/local/nagios/etc/nagios.cfg"

PIDFILE = /usr/local/nagios/var/$NAME.lock

**Step 18**: Make the Nagios file executable and start Nagios.

*sudo chmod +x /etc/init.d/Nagios*

*service apache2 restart*

*service nagios start*

**Step 19**: Now go to the browser and open url: **http://localhost/nagios**. Login to Nagios with username nagiosadmin and use the password which had been set earlier.

**Step 20:** Install NRPE Plugin in Nagios

Go to the nagios download directory and download the latest NRPE Plugin or use the following wget command.

*wget https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-4.0.2/nrpe-4.0.2.tar.gz*

Unpack the NRPE source code tarball.

*tar xzf nrpe-4.0.2.tar.gz*

*cd nrpe-4.0.2*

Compile and install the NRPE addon.

*./configure*

*make all*

*make install-plugin*

*make install-daemon*

*make install-init*

**Step 21:** Verify NRPE Daemon Remotely

Make sure that the check\_nrpe plugin can communicate with the NRPE daemon on the remote Linux host. Add the IP address in the command below with the IP address of the monitored Remote Linux host.

*/usr/local/nagios/libexec/check\_nrpe -H* 192.168.12.135

* **Set up windows server 2019 (Windows client):** Download NSClient++

*http://nsclient.com/download/*

* **Set up Ubuntu 16.04.7 (Linux client):** Download NRPE

Install the NRPE (Nagios Remote Plugin Executor) server and Nagios plugins

*sudo apt-get install nagios-nrpe-server nagios-plugins*

* 1. **Configuration**
* **Configuration of Nagios Monitoring Server (Ubuntu 16.04.7):**

**Step 1:** Open the winserver.cfg and add the new host definition for the windows machine which is being monitored.

*nano /usr/local/nagios/etc/servers/winserver.cfg*

The address of host is IP address of window server that is monitored



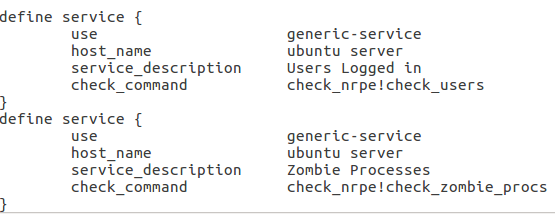


**Step 2:** Open the ubuntu.cfg and add the new host definition for the ubuntu machine which is being monitored.

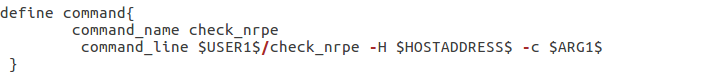
*nano /usr/local/nagios/etc/servers/ubuntu.cfg*

The address of host is IP address of ubuntu machine that is monitored





**Step 3:** Add command for check\_nrpe into file /usr/local/nagios/etc/objects/commands.cfg



**Step 4:** Restart the NRPE service on a system that uses systemd for service management

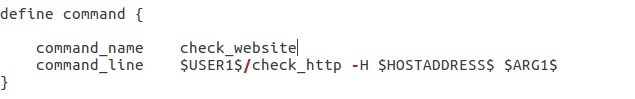
*sudo systemctl restart nagios*

**Step 5:** Create and open the website.cfg and add the new host definition for the website which is being monitored.



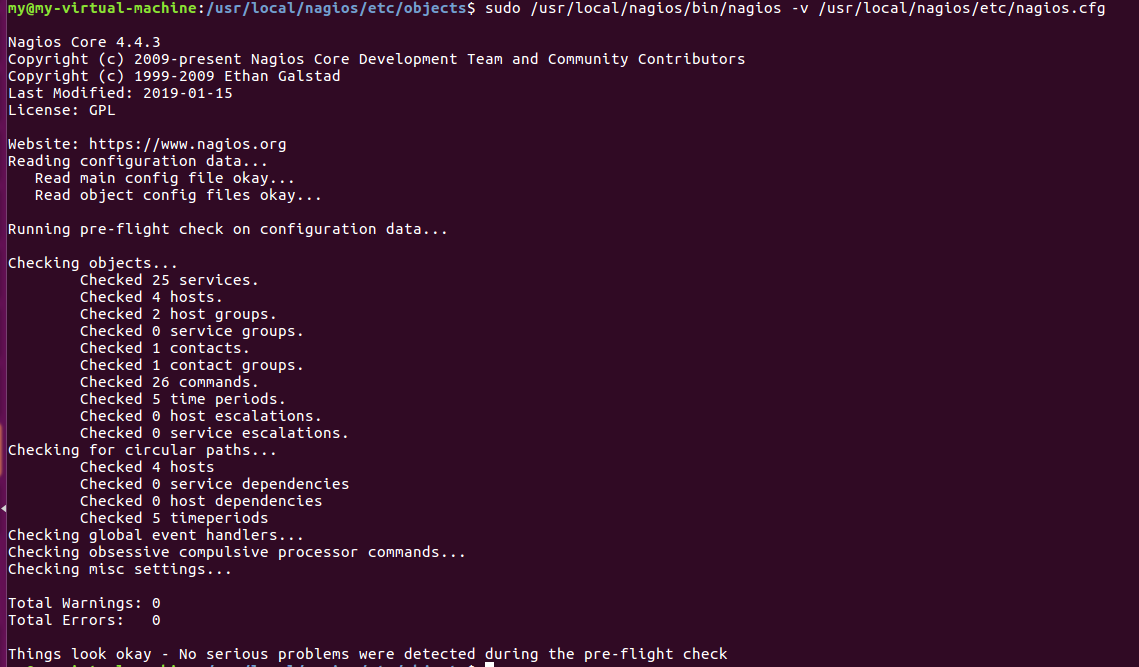
In this file, we monitored daa.uit.edu.vn

**Step 6:** Add command check\_website into commands.cfg



**Step 7:** Verify and restart nagios

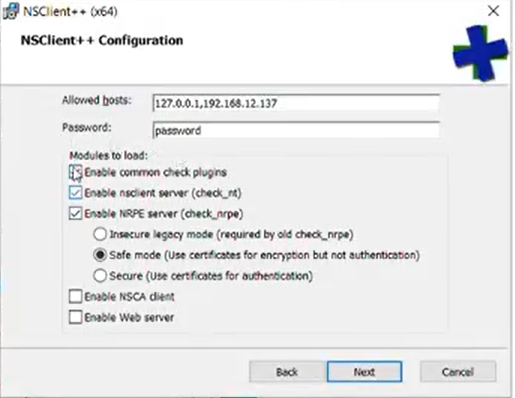
*sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg*



*systemctl status nagios.service*

* **Configuration of Windows client (Windows server 2019):**

**Step 1:** Add IP address of Nagios server into allowed-host.



**Step 2:** Open Notepad as Adminitrator and edit the NSClient++ configuration to enable the following modules:

*CheckExternalScripts = 1*

*CheckHelpers = 1*

*CheckEventLog = 1*

*CheckNSCP = 1*

*CheckDisk = 1*

*CheckSystem = 1*

* **Configuration of Linux client (Ubuntu 16.04.7):**

**Step 1:** Customize NRPE Commands

*cd /etc/nagios*

*gedit nrpe.cfg*

Add ip address of Nagios server machine into allowd-hosts



**Step 2:** Allow port 5666, as NRPE typically uses port 5666 for communication between the Nagios server and the NRPE client.

*sudo ufw allow 5666/tcp*

**Step 3:** Restart the NRPE service on a system that uses systemd for service management

*sudo systemctl restart nagios-nrpe-server*

1. **Results**

When monitoring a system with Nagios, there are various types of statuses used to describe the state of hosts and services in the monitoring environment. The key as follow:

Host States:

* UP: The host is functioning correctly and responds to checks.
* DOWN: The host is not responding to checks, indicating a potential issue like network connectivity problems.
* UNREACHABLE: Nagios cannot reach the host, often due to network issues.

Service States:

* OK: The service is operating normally, and its state is stable.
* WARNING: The service is experiencing issues that may require attention. Some minor problems may trigger a warning.
* CRITICAL: The service is in a critical state and needs immediate attention. This is a more severe state than WARNING.
* UNKNOWN: This state occurs when Nagios cannot determine the status of the service, often due to configuration errors or malfunctioning plugins.

Common States:

* PENDING: A temporary state while Nagios is awaiting confirmation of the status of a host or service after a change.
* DEPENDENT: The status of a host or service depends on the status of one or more other hosts or services.

Event States:

* ACKNOWLEDGED: The state of a host or service has been acknowledged, meaning that an administrator is aware of the issue and is handling it.
* SCHEDULED DOWNTIME: The host or service is in a scheduled downtime, during which Nagios will not generate alerts.

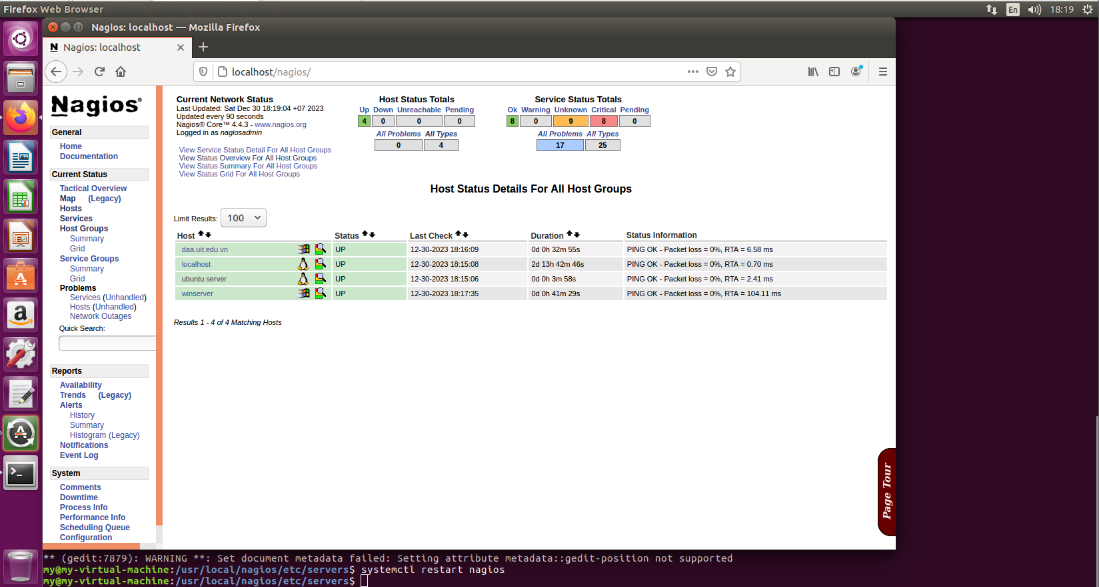
FLAPPING: The state of a host or service is oscillating between OK, WARNING, and CRITICAL in an unstable manner.

* 1. **Monitor Windows**

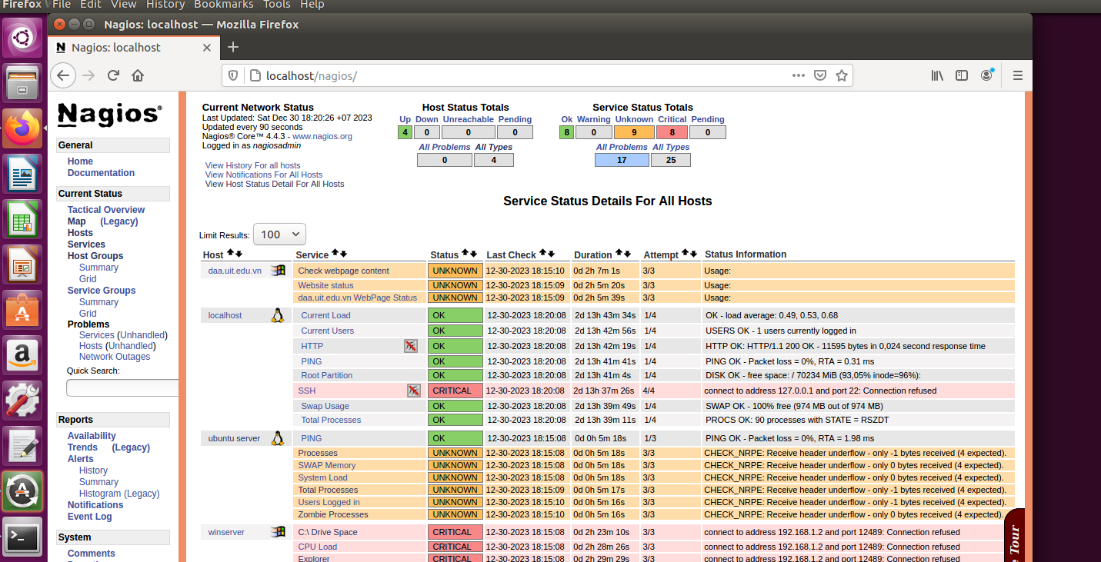
Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Description automatically generated

* 1. **Monitor Linux**



* 1. **Monitor Web Server**



1. **Demonstration**

Link: https://youtu.be/st2E-7Aq5ZA

1. **Appendix**
2. **Self-evaluation**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Report format | Theory | Presentation | Demonstration | Total Score |
| 1 | 2 | 1 | 5 | 9 |

1. **Task Assignment**

|  |  |  |
| --- | --- | --- |
| Member | Task | Task completion (%) |
| Bùi Hoàng Trúc Anh | Monitor Windows | 100% |
| Nguyễn Ngọc Trà My | Monitor Linux | 100% |
| Lê Hoàng Oanh | Monitor Web Server | 100% |

1. **Q&A**

|  |  |
| --- | --- |
| Questions | Answers |
| Can Nagios monitor others network device such as a switch or a router? | Yes, Nagios is designed to monitor a wide range of network devices, including switches and routers. Nagios achieves this through its extensible plugin architecture. Users can create or leverage existing plugins that support specific protocols or methods for querying the status and performance of network devices.  Commonly used plugins for monitoring switches and routers include SNMP (Simple Network Management Protocol) plugins. SNMP is a standard protocol for monitoring and managing devices on IP networks. Nagios plugins can use SNMP queries to retrieve information such as interface status, bandwidth usage, error rates, and other relevant metrics. |
| Nagios có thể phát hiện host bất thường hay không? | Nagios has the ability to detect unusual hosts through monitoring and checking them. Anomaly hosts often include unexpected states such as interruptions in service, lost connections, or tampering. |
| What is a Nagios plugin, and how does it work? | A Nagios plugin is a script or executable that performs specific checks on hosts or services. Nagios uses scheduled check commands, associating them with monitored items. Plugins are executed at intervals, reporting results through return codes and optional performance data. These results are processed by Nagios to trigger notifications based on configured thresholds. Plugins make Nagios highly adaptable and extensible for monitoring diverse devices and services in a network. |
| How does Nagios handle notifications when a service or host goes down? | Nagios handles notifications through a configurable system involving contacts, contact groups, and notification commands. Contacts are assigned to hosts or services, and notification settings, including intervals and escalation, are defined for each contact. When a service or host enters a non-okay state, Nagios sends notifications based on the configured settings, using methods such as email, SMS, or custom scripts. This flexibility allows administrators to tailor the notification behavior to match the organization's requirements and response procedures. |
| How to fix SSH critical error on server side | This error occurs because the SSH service on the server has not been installed yet. Installing the SSH service on the server will solve the problem. |
| How to fix services with UNKNOWN errors on clients? | To fix services with UNKNOWN errors in Nagios:  1. Check plugin output and logs for more details.  2. Ensure plugins are up-to-date.  3. Verify resource usage on the monitored server.  4. Check for network connectivity issues.  5. Verify permissions on plugin files.  6. Review Nagios configuration for errors.  7. Test connectivity from Nagios server to client.  8. Check for service dependencies.  9. Refer to plugin-specific documentation.  10. Restart Nagios services if needed. |
| How many devices can Nagios monitor at one time? | The number of devices that Nagios can monitor at one time depends on several factors, including the hardware resources of the Nagios server, the frequency of checks, and the complexity of the monitoring tasks. Nagios itself doesn't have a hard-coded limit on the number of devices it can monitor, but practical limits are determined by the server's processing power, memory, and network capacity.  For small to medium-sized installations, Nagios can effectively monitor hundreds to a few thousand devices. In larger environments, administrators may need to distribute the monitoring load by using multiple Nagios servers or implementing distributed monitoring solutions. |
| Nagios có hữu dụng khi dùng trong quy mô lớn, có live data như Grafana | Both Nagios and Grafana can be combined to get the combination of real-time alerts from Nagios and the visualization and detailed analytics capabilities from Grafana. Grafana can be used to visualize monitoring data from Nagios, making it a powerful visualization interface. |
| Nhóm bạn sử dụng biểu đồ, đồ thị hay dashboard không để theo dõi trạng thái hệ thống? | In Nagios there is PnP4Nagios addon which is used to provide visualization of monitoring data from Nagios. PnP4Nagios helps create charts and reports based on current and historical data from Nagios, making performance monitoring and analysis easier and more intuitive. |
| Làm sao để tối ưu hóa Nagios để đáp ứng nhu cầu trong thực tế (doanh nghiệp) | To optimize Nagios to meet the needs of an enterprise environment, the following steps should be taken:   * Smart Configuration Management: Organize configurations logically and use templates. Periodically review and update configuration. * Selective Monitoring: Focus on critical services and adjust inspection intervals accordingly. * Collect and Analyze Performance Data: Enable performance data and use visualization tools to analyze trends. * Effective Alerts: Fine-tune alert thresholds to avoid spurious notifications. Implement enhanced policy to ensure timely response. * Notification Enhancement: Use multiple notification channels and group related notifications. * High Availability (HA) Setup: Deploy Nagios in a highly available environment with redundant configurations. * Periodically Test and Adjust: Periodically evaluate and adjust configurations based on changing business requirements. * Documentation and Training: Keep documentation clear and provide training on Nagios best practices. * Integration with Other Systems: Integrate Nagios with ITSM tools to manage incidents and implement process automation to achieve effective response. |