* 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*

Giải thích

* sudo: Là một lệnh trong Linux, cho phép người dùng thực thi lệnh với đặc quyền quản trị (root) mà không cần phải đăng nhập vào tài khoản root.
* apt-get: Là trình quản lý gói trong hệ điều hành Ubuntu. Nó được sử dụng để cài đặt, cập nhật và gỡ cài đặt các gói phần mềm.
* install: Là tham số của apt-get, được sử dụng để cài đặt các gói phần mềm.
* wget: Là công cụ dòng lệnh để tải xuống dữ liệu từ internet. Trong trường hợp này, nó có thể được sử dụng để tải xuống các tệp tin cần thiết cho việc cài đặt Nagios Core.
* build-essential: Là một gói phần mềm chứa các công cụ cần thiết để biên dịch và cài đặt phần mềm từ mã nguồn. Trong trường hợp này, nó cần thiết để biên dịch mã nguồn của Nagios Core.
* apache2: Là máy chủ web Apache, một máy chủ web phổ biến được sử dụng để chạy các ứng dụng web.
* php: Là một ngôn ngữ lập trình phía máy chủ thường được sử dụng để phát triển ứng dụng web. Apache cần được cấu hình để hỗ trợ PHP để chạy Nagios Core.
* apache2-mod-php7.0: Là một mô-đun cho Apache để kết nối với PHP 7.0.
* php-gd: Là một thư viện hỗ trợ trong PHP cho việc xử lý đồ họa, có thể cần cho các tính năng đồ họa trong Nagios Core.
* libgd-dev: Là gói phát triển của thư viện GD, một thư viện đồ họa cho xử lý hình ảnh. Cần thiết nếu bạn muốn sử dụng các tính năng liên quan đến đồ họa trong Nagios Core.
* sendmail: Là một chương trình gửi thư trong hệ thống Linux. Nagios thường sử dụng nó để gửi thông báo qua email.
* unzip: Là một tiện ích để giải nén các tệp tin nén. Có thể sử dụng nó để giải nén các tệp tin tải xuống từ internet.

**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*

Giải thích

Câu lệnh trên được sử dụng để tạo người dùng và nhóm cần thiết cho Nagios và đảm bảo rằng chúng được thêm vào nhóm người dùng Apache www-data. Dưới đây là giải thích chi tiết:

* sudo useradd nagios: Tạo một người dùng có tên là "nagios". Người dùng này sẽ được sử dụng để chạy các dịch vụ và quy trình của Nagios.
* sudo groupadd nagcmd: Tạo một nhóm có tên là "nagcmd". Nhóm này sẽ được sử dụng để quản lý quyền truy cập và điều khiển các lệnh của Nagios.
* sudo usermod -a -G nagcmd nagios: Thêm người dùng "nagios" vào nhóm "nagcmd". Điều này đảm bảo rằng người dùng "nagios" có đủ quyền để thực hiện các lệnh và thao tác liên quan đến Nagios.
* sudo usermod -a -G nagios,nagcmd www-data: Thêm người dùng www-data (người dùng mặc định của Apache) vào cả hai nhóm "nagios" và "nagcmd". Điều này làm cho Apache có thể truy cập các tệp và thư mục cần thiết để chạy Nagios Core mà không gặp phải các vấn đề về quyền hạn.

Những bước này giúp xác định các người dùng và nhóm với đủ quyền để Nagios Core có thể chạy mà không gặp vấn đề về quyền hạn. Cụ thể, quy trình Nagios thường chạy với quyền của người dùng "nagios" và thuộc nhóm "nagcmd", trong khi Apache (www-data) được thêm vào nhóm này để có thể truy cập và thực hiện các lệnh của Nagios một cách an toàn.

**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*

Giải thích

Câu lệnh `./configure --with-nagios-group=nagios --with-command-group=nagcmd` được sử dụng trong quá trình biên dịch mã nguồn của Nagios. Dưới đây là giải thích chi tiết về các thành phần trong câu lệnh này:

* ./configure: Là một script cấu hình tự động thường đi kèm với mã nguồn của nhiều ứng dụng mã nguồn mở. Nó được sử dụng để cấu hình mã nguồn để phù hợp với môi trường cụ thể của hệ thống.
* --with-nagios-group=nagios: Tham số này chỉ định nhóm người dùng mà quy trình Nagios sẽ sử dụng khi chạy. Trong trường hợp này, quy trình Nagios sẽ chạy với quyền của nhóm "nagios", giúp đảm bảo rằng nó có quyền truy cập đến các tệp và thư mục cần thiết.
* --with-command-group=nagcmd: Tham số này chỉ định nhóm người dùng mà các lệnh của Nagios sẽ sử dụng. Các lệnh của Nagios thường được thực thi qua giao diện dòng lệnh và thường cần quyền truy cập đặc biệt để thực hiện các hành động như thực hiện các lệnh cấu hình. Nhóm "nagcmd" đảm bảo rằng các lệnh này có đủ quyền.

Các tham số này đảm bảo rằng Nagios Core được cấu hình để chạy với các quyền hạn cụ thể, giúp đảm bảo tính an toàn và bảo mật của hệ thống. Nó cũng giúp quản trị viên kiểm soát quyền truy cập và thực hiện các tác vụ quản lý Nagios một cách hiệu quả.

**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*

Giải thích

* sudo make install-commandmode: Lệnh này thường được sử dụng để cài đặt các tệp và thư mục cần thiết để chạy Nagios Core với quyền hạn thực thi (execute permissions) cho các lệnh của Nagios. Cụ thể, nó cài đặt các tệp và thư mục cần thiết để quy trình Nagios có thể thực hiện các lệnh cấu hình và quản lý.
* sudo make install-init: Lệnh này thường được sử dụng để cài đặt các tệp cấu hình để Nagios Core có thể được quản lý như một dịch vụ (service) trên hệ thống. Cụ thể, nó có thể cài đặt các tệp init.d hoặc systemd để khởi động và dừng Nagios như một dịch vụ.
* sudo make install-config: Lệnh này thường được sử dụng để cài đặt các tệp cấu hình mẫu và các tệp cấu hình cơ bản cho Nagios Core. Cụ thể, nó có thể cài đặt các tệp như nagios.cfg, cgi.cfg, resource.cfg, và các tệp khác cần thiết để cấu hình Nagios.
* sudo /usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-available/nagios.conf: Lệnh này được sử dụng để cài đặt tệp cấu hình Apache để Nagios có thể được truy cập qua giao diện web. Trong trường hợp này, tệp cấu hình được sao chép từ sample-config/httpd.conf và được đặt trong thư mục cấu hình của Apache (/etc/apache2/sites-available/) với tên là 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*

Giải thích

Câu lệnh `sudo cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/` và `sudo chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers` được sử dụng để sao chép thư mục event handler (bộ xử lý sự kiện) và đảm bảo rằng nó thuộc quyền sở hữu của người dùng và nhóm "nagios". Dưới đây là giải thích chi tiết về từng bước:

* sudo cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/: Lệnh này sao chép thư mục `eventhandlers` từ thư mục `contrib` vào thư mục `libexec` trong cài đặt Nagios. Thư mục `libexec` thường chứa các script và plugin được sử dụng bởi Nagios để thực hiện các chức năng cụ thể. Trong trường hợp này, thư mục `eventhandlers` chứa các script dùng để xử lý sự kiện (event) khi Nagios phát hiện ra vấn đề.
* sudo chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers: Lệnh này đặt quyền sở hữu của thư mục `eventhandlers` thành người dùng và nhóm "nagios". Việc này là quan trọng để đảm bảo rằng quy trình Nagios, chạy dưới tên người dùng "nagios", có quyền truy cập và thực thi các script trong thư mục `eventhandlers`.

Bước này giúp Nagios có thể sử dụng các event handler một cách hiệu quả khi có sự kiện xảy ra, giúp tăng cường khả năng tự động hóa và xử lý sự cố. Các event handler thường được sử dụng để thực hiện các hành động cụ thể khi một vấn đề được phát hiện, chẳng hạn như gửi thông báo, khởi động lại dịch vụ, hoặc thực hiện các biện pháp khác để giải quyết sự cố.

**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*

Giải thích

Bước này liên quan đến việc cài đặt Nagios Plugins, một bộ sưu tập các tiện ích mà Nagios sử dụng để kiểm tra và giám sát các tài nguyên khác nhau trên hệ thống. Dưới đây là giải thích chi tiết về từng thành phần trong các câu lệnh:

* ./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl: Câu lệnh này được sử dụng để cấu hình quá trình biên dịch của Nagios Plugins. Cụ thể:
* --with-nagios-user=nagios và --with-nagios-group=nagios: Xác định người dùng và nhóm mà Nagios Plugins sẽ sử dụng khi chạy. Trong trường hợp này, nó được cấu hình để sử dụng người dùng và nhóm "nagios", đảm bảo rằng plugins sẽ chạy với các quyền hạn thích hợp.
* --with-openssl: Cung cấp hỗ trợ cho OpenSSL, một thư viện mã nguồn mở được sử dụng để thực hiện các chức năng mã hóa và bảo mật. Trong trường hợp này, OpenSSL có thể được sử dụng cho các plugin liên quan đến mã hóa và bảo mật.
* make: Lệnh này sẽ biên dịch mã nguồn của Nagios Plugins sau khi đã được cấu hình.
* sudo make install: Câu lệnh này sẽ cài đặt Nagios Plugins đã được biên dịch vào hệ thống. Những plugins này có thể bao gồm các ứng dụng như check\_http để kiểm tra trạng thái của máy chủ web, check\_disk để kiểm tra trạng thái của ổ đĩa, và nhiều loại kiểm tra khác để đảm bảo rằng các dịch vụ và tài nguyên hệ thống hoạt động đúng cách.

Việc cài đặt Nagios Plugins là quan trọng để Nagios có thể thực hiện các kiểm tra và giám sát đa dạng trên hệ thống. Các plugins này cung cấp các chức năng kiểm tra cụ thể để đảm bảo rằng tất cả các thành phần của hệ thống đang hoạt động đúng cách và có sẵn cho quá trình giám sát của Nagios.

**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

Giải thích

Loại bỏ ký tự chú thích (#) từ dòng 51, giúp bật chức năng sử dụng thư mục cấu hình servers.

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

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

Giải thích

Tạo thư mục để chứa các tệp cấu hình cho các máy chủ cụ thể mà Nagios sẽ giám sát.

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

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

Giải thích

Bạn cần thay đổi địa chỉ email thành địa chỉ thực tế của người dùng để có thể nhận được thông báo từ Nagios khi có sự cố xảy ra.

**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/*

Giải thích

Bước này liên quan kích hoạt các module Apache và cấu hình một người dùng là nagiosadmin. Dưới đây là giải thích chi tiết về từng thành phần trong các câu lệnh:

* sudo a2enmod rewrite: Bật module rewrite của Apache. Module rewrite là một module của Apache giúp xử lý việc chuyển hướng URL và tái chế URL (URL rewriting). Trong trường hợp của Nagios, việc này là quan trọng để có thể định tuyến các yêu cầu HTTP đến các trang và tài nguyên cụ thể.
* sudo a2enmod cgi: Bật module CGI của Apache. Module CGI là một phần quan trọng để thực hiện giao tiếp giữa máy chủ web và các ứng dụng khác nhau. Trong trường hợp Nagios, việc này là cần thiết để có thể chạy các script CGI mà Nagios sử dụng để hiển thị thông tin trên giao diện web.
* sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin: Tạo một tệp htpasswd để quản lý người dùng và mật khẩu cho trang web bảo mật của Nagios. Lệnh này sử dụng chương trình htpasswd để tạo và quản lý tệp password. Trong trường hợp này, một người dùng có tên là "nagiosadmin" được tạo ra và thông tin đăng nhập của họ được lưu trữ trong tệp htpasswd. Khi người dùng truy cập trang web Nagios, họ sẽ cần nhập thông tin đăng nhập để xác thực.
* sudo ln -s /etc/apache2/sites-available/nagios.conf /etc/apache2/sites-enabled/: Tạo một liên kết tượng trưng từ sites-available đến sites-enabled, để Apache có thể sử dụng cấu hình của Nagios. Liên kết này là cần thiết để Apache biết nơi để tìm cấu hình của trang web Nagios. Nó giúp kích hoạt cấu hình từ sites-available, cho phép Nagios hoạt động dưới sự kiểm soát của Apache.

**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*

Giải thích

Những bước này giúp đảm bảo rằng Apache và Nagios được khởi động và cấu hình đúng cách sau khi bạn đã thực hiện các bước trước đó trong quá trình cài đặt Nagios Core.

* service apache2 restart: Làm mới dịch vụ Apache để áp dụng các thay đổi cấu hình mới, bao gồm việc kích hoạt module và cấu hình cho Nagios.
* service nagios start: Khởi động dịch vụ Nagios. Sau khi đã cài đặt và cấu hình, bạn cần bắt đầu chạy Nagios để nó có thể theo dõi và giám sát hệ thống.
* cd /etc/init.d/: Di chuyển đến thư mục init.d. Thường thì các script init.d chứa các tệp tin cấu hình cho các dịch vụ hệ thống.
* sudo cp /etc/init.d/skeleton /etc/init.d/Nagios: Sao chép tệp mẫu (skeleton) để tạo một script init.d tùy chỉnh cho dịch vụ Nagios. Việc này có thể là bước chuẩn bị cho việc tự động hóa quá trình khởi động Nagios khi hệ thống khởi động.

**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

Giải thích

Bước này là để tạo một script init.d tùy chỉnh (trong trường hợp này là Nagios) để quản lý việc khởi động, dừng, và quản lý dịch vụ Nagios. Nó giúp hệ thống biết cách thực hiện các hành động với dịch vụ Nagios như khởi động tự động khi hệ thống khởi động.

* DESC="Nagios": Mô tả dịch vụ Nagios, thông tin này sẽ được hiển thị khi thực hiện các lệnh hệ thống liên quan đến dịch vụ.
* NAME=nagios: Đặt tên cho dịch vụ, ở đây là "nagios".
* DAEMON=/usr/local/nagios/bin/$NAME: Đường dẫn đến chương trình chính của Nagios.
* DAEMON\_ARGS="-d /usr/local/nagios/etc/nagios.cfg": Các tham số được truyền cho chương trình Nagios khi nó được khởi động. Trong trường hợp này, -d là để chạy Nagios ở chế độ nền (daemon mode), và đường dẫn đến tệp cấu hình nagios.cfg.
* PIDFILE=/usr/local/nagios/var/$NAME.lock: Đường dẫn đến tệp tin nơi sẽ lưu ID quá trình (PID) của Nagios khi nó đang chạy.

**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.

*cd /root/nagios*

*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*

Giải thích

Bước này là quan trọng để mở rộng khả năng giám sát của Nagios đến các máy chủ từ xa và theo dõi các dịch vụ và tài nguyên trên chúng. NRPE đóng vai trò quan trọng trong việc thực hiện giám sát phức tạp và chi tiết trên nhiều máy chủ.

* Configure, build, và cài đặt NRPE addon: Các bước này thực hiện việc cấu hình, biên dịch, và cài đặt NRPE addon vào hệ thống Nagios. Các bước này đảm bảo rằng NRPE sẽ hoạt động và sẵn sàng để chấp nhận các plugin từ Nagios để thực hiện giám sát từ xa.

**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 <remote\_linux\_ip\_address> đổi lại thành địa chỉ ip của Linux client*

* **Set up windows server 2019 (Windows client):** Download NSClient++
* **Set up Ubuntu 16.04.7 (Linux client):** Download NRPE

Giải thích

Bước này giúp xác minh rằng Nagios có thể kết nối và giao tiếp với NRPE daemon trên máy chủ Linux từ xa mà bạn muốn giám sát. Điều này là quan trọng để đảm bảo rằng plugin NRPE được cài đặt và hoạt động đúng cách trên máy chủ từ xa.Việc kiểm tra này giúp xác định xem Nagios có thể nhận thông tin giám sát từ các máy chủ từ xa thông qua NRPE hay không. Điều này là cơ sở cho việc cấu hình các mục giám sát cụ thể cho các máy chủ và dịch vụ trên chúng.

* Bước này giúp xác minh rằng Nagios có thể kết nối và giao tiếp với NRPE daemon trên máy chủ Linux từ xa mà bạn muốn giám sát. Điều này là quan trọng để đảm bảo rằng plugin NRPE được cài đặt và hoạt động đúng cách trên máy chủ từ xa.
* Việc kiểm tra này giúp xác định xem Nagios có thể nhận thông tin giám sát từ các máy chủ từ xa thông qua NRPE hay không. Điều này là cơ sở cho việc cấu hình các mục giám sát cụ thể cho các máy chủ và dịch vụ trên chúng.

Bước này là cần thiết để cấu hình giám sát từ xa từ Nagios đối với cả các máy chủ Windows và Linux, mở rộng khả năng giám sát của hệ thống

* Cài đặt Windows Server 2019 (Windows client) Download NSClient++: Chuẩn bị cài đặt NSClient++ trên máy chủ Windows để cho phép Nagios giám sát máy chủ này. NSClient++ là một agent giám sát cho hệ điều hành Windows, cho phép Nagios giám sát các dịch vụ và tài nguyên trên máy chủ Windows. Cài đặt này là quan trọng để mở rộng khả năng giám sát của Nagios đến các máy chủ chạy hệ điều hành Windows.
* Cài đặt Ubuntu 16.04.7 (Linux client) Download NRPE: Chuẩn bị cài đặt NRPE trên máy chủ Linux để cho phép Nagios giám sát máy chủ này. NRPE (Nagios Remote Plugin Executor) cho phép Nagios giám sát các dịch vụ và tài nguyên trên máy chủ Linux từ xa. Cài đặt này mở rộng khả năng giám sát của Nagios đến các máy chủ chạy hệ điều hành Linux.

**Step 22:** Install Required Dependencies: We need to install required libraries like gcc, glibc, glibc-common, and GD and its development libraries using the yum package manager.

*sudo apt install -y gcc glibc glibc-common gd gd-devel make net-snmp openssl-devel tar wget*

Giải thích

* gcc: Compiler cho việc biên dịch mã nguồn C. Trong trường hợp Nagios, đây là một phần quan trọng để biên dịch mã nguồn và các plugin.
* glibc và glibc-common: Thư viện C tiêu chuẩn. Glibc là thư viện C cơ bản, còn glibc-common là các tệp và tài liệu chung cho Glibc. Cả hai đều là phần quan trọng của môi trường thực thi của Nagios.
* gd và gd-devel: Thư viện GD là một thư viện đồ họa đa dụng. GD-devel cung cấp các tệp và thư viện phát triển cần thiết để sử dụng GD trong các ứng dụng và plugin của Nagios.
* make: Công cụ biên dịch dựa trên Makefile. Được sử dụng để tự động hóa quy trình biên dịch.
* net-snmp: Thư viện SNMP cho phép Nagios giám sát và thu thập thông tin từ các thiết bị mạng.
* openssl-devel: Thư viện và các công cụ phát triển cho OpenSSL. Cần thiết để hỗ trợ HTTPS và SSL khi Nagios giao tiếp với các thiết bị khác.
* tar và wget: Các công cụ cần thiết để giải nén và tải xuống mã nguồn từ các nguồn trực tuyến.

**Step 22:** Create Nagios User: Create a new nagios user account and set a password.

*useradd nagios*

*passwd nagios*

**Step 24:** Install the Nagios Plugins: Create a directory for nagios plugin installation and all its future downloads.

*mkdir /root/nagios*

*cd /root/nagios*

*wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz*

**Step 25:** Extract Nagios Plugins: Run the following tar command to extract the source code tarball.

*tar -xvf nagios-plugins-2.3.3.tar.gz*

**Step 26:** Compile and Install Nagios Plugins: Next, compile and install nagios plugins using the following commands

*cd nagios-plugins-2.3.3*

*./configure*

*make*

*make install*

Set the permissions on the plugin directory using the chown command.

*chown nagios.nagios /usr/local/nagios*

*chown -R nagios.nagios /usr/local/nagios/libexec*

Giải thích

chown nagios.nagios /usr/local/nagios:

* /usr/local/nagios là thư mục chính của Nagios Core.
* chown nagios.nagios sẽ thay đổi người sở hữu của thư mục này thành nagios và nhóm sở hữu thành nagios. Điều này đảm bảo rằng Nagios Core có quyền truy cập và thực thi các tệp tin trong thư mục này với quyền của người dùng và nhóm nagios.

chown -R nagios.nagios /usr/local/nagios/libexec:

* /usr/local/nagios/libexec là thư mục chứa các tệp thực thi (plugins) của Nagios.
* chown -R nagios.nagios sẽ thay đổi người sở hữu và nhóm sở hữu của thư mục và tất cả các tệp tin bên trong (do có tùy chọn -R, có nghĩa là đệ quy) thành nagios và nagios. Điều này đảm bảo rằng Nagios Core có quyền thực thi các plugins mà nó sử dụng để kiểm tra trạng thái của các máy chủ và dịch vụ.

**Step 27:** Installing NRPE Plugin: To install the nrpe plugin, first, download the latest NRPE Plugin or use the following wget command.

*cd /root/nagios*

*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*

Next, install the NRPE plugin daemon, and sample config files.

*make install-plugin*

*make install-daemon*

*make install-config*

Install the NRPE daemon under systemd as a service.

*make install-init*

**Step 28:** Configuring NRPE Plugin: Now open /usr/local/nagios/etc/nrpe.cfg file and add the local host and IP address of the Nagios Monitoring Server.

*allowed\_hosts=127.0.0.1,192.168.102*

Next, enable and restart the nrpe service.

*systemctl enable nrpe*

*systemctl restart nrpe*

Giải thích

Bước này cấu hình NRPE để chấp nhận yêu cầu từ localhost và địa chỉ IP của máy chủ Nagios Monitoring. Điều này là quan trọng để bảo mật NRPE và ngăn chặn việc sử dụng không được phép từ các nguồn không an toàn. Kích hoạt và khởi động lại dịch vụ NRPE để áp dụng cấu hình mới và đảm bảo rằng NRPE sẵn sàng để giao tiếp với Nagios Monitoring Server.

* allowed\_hosts: Thêm địa chỉ IP của localhost và địa chỉ IP của máy chủ Nagios Monitoring vào danh sách allowed\_hosts. Điều này cho phép NRPE chấp nhận yêu cầu từ những địa chỉ IP này. Điều này là quan trọng để bảo vệ NRPE khỏi việc bị sử dụng mà không được phép từ các nguồn không an toàn.
* systemctl enable nrpe: Kích hoạt dịch vụ NRPE để nó tự động khởi động khi hệ thống khởi động.
* systemctl restart nrpe: Khởi động lại dịch vụ NRPE để áp dụng các thay đổi cấu hình mới. Việc này cần thiết để NRPE nhận biết và chấp nhận các yêu cầu từ Nagios Monitoring Server.

**Step 29:** Open NRPE Port in Firewall

Make sure that the Firewall on the local machine will allow the NRPE daemon to be accessed from remote servers. To do this, run the following iptables command.

*firewall-cmd --zone=public --add-port=5666/tcp*

*firewall-cmd --zone=public --add-port=5666/tcp --permanent*

Giải thích

NRPE sử dụng cổng 5666 để giao tiếp với Nagios Monitoring Server từ xa. Việc mở cổng này trong tường lửa là quan trọng để cho phép NRPE nhận yêu cầu từ Nagios. Bước này giúp đảm bảo rằng NRPE có thể kết nối và truyền thông với Nagios Monitoring Server qua mạng, mở rộng khả năng giám sát từ xa của Nagios.

* firewall-cmd: Là một công cụ quản lý tường lửa trên các hệ thống sử dụng Firewalld.
* --zone=public: Xác định khu vực trong tường lửa, ở đây là khu vực công cộng.
* --add-port=5666/tcp: Thêm cổng 5666 với giao thức TCP vào tường lửa.
* --permanent: Làm cho thay đổi cấu hình trở thành vĩnh viễn, sẽ được áp dụng sau khi hệ thống khởi động lại.

**Step 30:** Verify NRPE Daemon Locally

Run the following netstat command to verify the NRPE daemon working correctly under systemd.

*netstat -at | grep nrpe*

Next, verify the NRPE daemon is functioning properly by running the “check\_nrpe” command that was installed earlier for testing purposes.

*/usr/local/nagios/libexec/check\_nrpe -H 127.0.0.1*

Giải thích

Bước này để kiểm tra trạng thái NRPE daemon thông qua netstat để đảm bảo rằng nó đang lắng nghe trên cổng mà Nagios sẽ sử dụng để gửi yêu cầu giám sát. Sử dụng lệnh check\_nrpe để kiểm tra khả năng làm việc của NRPE daemon. Lệnh này gửi yêu cầu kiểm tra cơ bản tới NRPE daemon và kiểm tra xem nó có thể xử lý yêu cầu đó và trả về kết quả hay không.

* netstat -at: Hiển thị trạng thái các kết nối TCP.
* grep nrpe: Lọc kết quả để chỉ hiển thị các dòng chứa từ "nrpe". Điều này giúp xác định xem NRPE daemon đang lắng nghe trên cổng mong muốn hay không.
* /usr/local/nagios/libexec/check\_nrpe -H 127.0.0.1: Chạy lệnh kiểm tra NRPE trên localhost để đảm bảo rằng NRPE daemon đang hoạt động đúng cách và có thể xử lý các yêu cầu từ Nagios.
  1. **Configuration**
* **Configuration of Nagios Monitoring Server (Ubuntu 16.04.7):**

**Step 1:** Enter Ubuntu root account.

*sudo -i*

**Step 2:** Open the nagios.cfg and uncomment line 38 which is the cfg\_file of Definitions for monitoring a Windows machine.

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

**Step 3:** Open the windows.cfg and add the new host definition for the windows machine which is being monitored.

*nano /usr/local/nagios/etc/objects/windows.cfg*

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

Description automatically generated

**Step 4:** Creating Nagios Host and Services File

*cd /usr/local/nagios/etc/*

*touch hosts.cfg*

*touch services.cfg*

Now add these two files to the main Nagios configuration file. Open the nagios.cfg file with any editor.

*vi /usr/local/nagios/etc/nagios.cfg*

Now add the two newly created files as shown below.

*cfg\_file=/usr/local/nagios/etc/hosts.cfg*

*cfg\_file=/usr/local/nagios/etc/services.cfg*

Giải thích

Bước này để tạo và quản lý tệp hosts.cfg và services.cfg giúp tổ chức và định nghĩa các máy chủ và dịch vụ mà Nagios sẽ giám sát. Bằng cách thêm hai tệp này vào tệp cấu hình chính, Nagios biết nơi tìm kiếm để lấy thông tin về hosts và services cần giám sát. Điều này giúp quá trình cấu hình trở nên dễ dàng và hiệu quả.

* touch hosts.cfg và touch services.cfg: Tạo hai tệp để chứa định nghĩa cho hosts (máy chủ) và services (dịch vụ) mà Nagios sẽ giám sát.
* cfg\_file=/usr/local/nagios/etc/hosts.cfg và cfg\_file=/usr/local/nagios/etc/services.cfg: Thêm đường dẫn tới hai tệp vừa tạo vào tệp cấu hình chính của Nagios. Điều này thông báo Nagios biết nơi để tìm kiếm định nghĩa hosts và services.

**Step 5:** Configuring Nagios Host and Services File

Now open hosts.cfg file and add the default host template name and define remote hosts as shown below. Make sure to replace host\_name, alias, and address with your remote host server details.

*vi /usr/local/nagios/etc/hosts.cfg*

Chỗ này thêm ảnh vào nha

Next open services.cfg file and add the following services to be monitored.

*vi /usr/local/nagios/etc/services.cfg*

Chỗ này thêm ảnh vào nha

**Step 6:** Configuring NRPE Command Definition

Now NRPE command definition needs to be created in commands.cfg file.

*vi /usr/local/nagios/etc/objects/commands.cfg*

Add the following NRPE command definition at the bottom of the file.

Chỗ này thêm ảnh vào nha

Verify Nagios Configuration files for any errors.

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

Finally, restart Nagios to apply recent configuration changes:

*systemctl restart nagios*

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

**Step 1:** 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*

**Step 2:** Restart the NSClient++ service on Windows 10

**Result:**

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

Description automatically generated

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

**Step 1:** Customize NRPE Commands

The default NRPE configuration file that got installed has several command definitions that will be used to monitor this machine. The sample configuration file is located at.

*vi /usr/local/nagios/etc/nrpe.cfg*

User can edit and add new command definitions by editing the NRPE config file. Finally, user’ve successfully installed and configu red NRPE agent on the Remote Linux Host.