TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

Viện Công nghệ Thông tin và Truyền thông

A close up of a sign

Description automatically generated

**BÁO CÁO BÀI TẬP LỚN**

**QUẢN TRỊ MẠNG**

Đề tài: **Nghiên cứu và triển khai giám sát hệ thống mạng bằng phần mềm mã nguồn mở Nagios**

GVHD: TS. Nguyễn Đức Toàn

Lớp: LTU15

Sinh viên: Nguyễn Đức Thiên

MSSV: 20168806

HN 05/2020

**Lời nói đầu**

Với tốc độ phát triển nhanh chóng cùng với sự tích hợp ngày càng nhiều các dịch vụ tiện ích, mạng máy tính ngày càng trở nên phức tạp và khó kiểm soát. Với một hệ thống thì việc giám sát các hoạt động là rất quan trọng bới nếu như có một sự cố xảy ra mà người quản trị không biết hoặc hệ thống không tự khắc phục thì sẽ ảnh hướng nghiêm trọng đến các doanh nghiệp. Vì vậy nhu cầu quản lý, giám sát hoạt động của mạng máy tính cũng như các dịch vụ của nó trở thành yêu cầu tất yếu. Rất nhiều phần mềm giám sát mạng đã được phát triển nhằm đáp ứng nhu cầu giám sát tự động các hệ thống mạng. Với một chi phi thấp và khả năng cấu hình linh hoạt, các phần mềm giám sát mạng mã nguồn mở là một lựa chọn tốt.

Trước những yêu cầu đó, em đã lựa chọn giải pháp triển khai phần mềm mã nguồn mở Nagio để thực hiện giám sát một mạng máy tính, không chỉ nhằm mục đích nghiên cứu mà còn nhằm phát triển, ứng dụng giám sát hệ thống mạng trong thực tiễn.

**MỤC LỤC**

[Chương 1. Phần mềm mã nguồn mở Nagios. 4](#_Toc43369111)

[1.1. Giới thiệu về Nagios. 4](#_Toc43369112)

[1.2. Cơ chế và kiến trúc hoạt động của Nagios. 4](#_Toc43369113)

[1.3. Hệ thống các tệp tin cấu hình. 5](#_Toc43369114)

[1.4. Triển khai và cấu hình Nagios trên Linux 7](#_Toc43369115)

[Chương 2. Thực nghiệm giám sát mạng với Nagios. 8](#_Toc43369116)

[2.1. Các dịch vụ giám sát 8](#_Toc43369117)

[2.2. Đánh giá hệ thống và kết quả đạt được 10](#_Toc43369118)

1. **Phần mềm mã nguồn mở Nagios.**
   1. Giới thiệu về Nagios.

* Nagios là một ứng dụng quản trị mạng nguồn mở, giám sát các máy trạm và các dịch vụ, cảnh báo khi có sự cố hoặc khi sự cố được khắc phục. Nagios được phát triển để chạy trên nền tảng Linux, có tính linh hoạt cao trong việc cấu hình các dịch vụ kiểm tra, các cấu hình có thể được đặt trong một file duy nhất hoặc đặt trong các file riêng lẻ cho từng thiết bị khác nhau, hay những mục đích khác nhau.
* Nagios cung cấp các cơ chế chính như giám sát tài nguyên hệ thống, tài nguyên mạng, dịch vụ mạng và các thông tin khác như nhiệt độ, thông báo, … Bên cạnh đó Nagios còn hỗ trợ giám sát từ xa thông qua SSH hay SSL.
* Nagios còn có khả năng thông báo cho người quản trị mạng khi các máy chủ hoặc dịch vụ gặp vấn đề, định nghĩa các xử lý sự kiện nhằm khắc phục sự cố tự động khi dịch vụ hoặc máy chủ gặp sự cố.
* Lưu trữ dữ liệu thông qua các tập tin văn bản thay vì cơ sở dữ liệu nào khác. Hỗ trợ người dùng với môi trường web-base cho phép theo dõi tình trạng mạng, các cảnh báo, sự cố …
  1. Cơ chế và kiến trúc hoạt động của Nagios.

Cơ chế hệ thống Nagios chia làm 2 phần cơ bản là:

* *Nagios Daemon:* làm nhiệm vụ chính là lập lịch kiểm tra định kỳ, nhận kết quả từ các Plugin gửi về và tiến hành phân tích kết quả, hiển thị trên giao diện Web hoặc thông báo tới người quản trị qua Email hoặc tin nhắn SMS.
* *Plugins:* làm nhiệm vụ chính là nhận điều khiển yêu cầu kiểm tra từ Daemon, thực thi các lệnh được yêu cầu, thu thập kết quả kiểm tra và gửi trả lại kết quả cho Daemon.

Ngoài ra Nagios còn cung cấp các Add-on để mở rộng phục vụ giám sát mạng cho các khía cạnh khác. Chẳng hạn như giám sát NRPE sử dụng dụng cho các máy chủ Linux , NSClient++ sử dụng cho giám sát các máy chủ Windows hoặc Nagiosgraph thực hiện thu thập số liệu và đưa ra các biểu đồ …

Đối với người quản trị mạng, Nagios cung cấp một giao diện web trực quan, dễ dàng giám sát và thực hiện một số thay đổi trong hệ thống.

A close up of text on a white background

Description automatically generated

Hình 1: Tương tác giữa các thành phần trong Nagios

Kiến trúc của hệ thống bao gồm các thành phần:

* *Nagios Core:* là thành phần chính của hệ thống, được thiết kế như một API, với các chức năng lập lịch kiểm tra và xử lí kết quả.
* *Cơ sở dữ liệu lưu trữ trạng thái:* Lưu trữ trạng thái của các thiết bị và dịch vụ được giám sát. Còn được sử dụng để lưu trữ thông tin trạng thái máy chủ khi khởi động lại.
* *Plugin:* Các phần mở rộng được cung cấp như một ứng dụng độc lập để thực thi các lệnh của Nagios.
* *Tệp tin cấu hình:* Những tệp tin định nghĩa các máy chủ, dịch vụ sẽ được giám sát.
* *Tệp tin nhật ký:* Lưu lại kết quả của việc kiểm tra, giám sát.
  1. Hệ thống các tệp tin cấu hình.

Hệ thống tập tin của Nagios rất đơn giản, các cấu hình được lưu dưới dạng tập tin \*.cfg, tập trung chủ yếu trong thư mục /usr/local/nagios/etc/ với các thành phần chính sau:

nagios.cfg: tập tin này chứa các thông tin trỏ tới các tập tin cấu hình khác, hoặc một thư mục chứa các tập tin cấu hình thông qua 2 chỉ thị cfg\_file và cfg\_dir. Điều này cung cấp tính linh hoạt cao cho Nagios.

resource.cfg: được dùng để lưu trữ các macro được định nghĩa bởi người dùng và nhừng thông tin cấu hình nhạy cảm như tên người dùng, mật khẩu …

cgi.cfg: (command gateway interface) lưu trữ các thông tin quan trọng của hệ thống cũng như định nghĩa các thành phần cơ bản như đường dẫn đến tập tin cấu hình chính nagios.cfg, tuỳ chỉnh các cách thức bảo mật cũng như truy cập vào hệ thống.

Ngoài 3 tập tin chính ở trên, Nagios còn có một số tập tin cfg lưu cấu hình mặc định cho các thiết bị, dịch vụ tương ứng trong thư mục objects như commands, contacts, localhost, printer, switch, templates, timeperiods, windows, để người dùng từ đó có thể mở rộng và tuỳ chỉnh các cấu hình phù hợp với hệ thống được giám sát.

A close up of text on a white background

Description automatically generated

Hình 2: Hệ thống các tệp tin cấu hình.

* 1. Triển khai và cấu hình Nagios trên Linux

Triển khai Nagios trên máy Thinkpad X1 Yoga gen 2.

Hệ điều hành: Ubuntu Desktop 18.04.4 LTS – 64bit

Processor Intel Core i7-7600U

Memory: 16GB

Disk: 512GB

Các bước triển khai Nagios Core trên máy chủ để giám sát hệ thống mạng:

* Cài đặt các gói cần thiết

$ sudo apt-get update  
 $ sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2 php libapache2-mod-php7.2 libgd-dev

* Tải về mã nguồn Nagios Core và thực hiện biên dịch.

$ cd /tmp  
 $ wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.5.tar.gz  
 $ tar xzf nagioscore.tar.gz

$ cd /tmp/nagioscore-nagios-4.4.5/

$ sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled

sudo make all

* Tạo người dùng nagios và group

$ sudo make install-groups-users  
 $ sudo usermod -a -G nagios www-data

* Biên dịch và thực hiện các cài đặt mặc định

$ sudo make install

$ sudo make install-daemoninit

$ sudo make install-commandmode

$ sudo make install-config

* Cài đặt và thiết lập một Apache webserver để chạy và giám sát Nagios thông qua giao diện web.

$ sudo make install-webconf

$ sudo a2enmod rewrite

$ sudo a2enmod cgi

$ sudo ufw allow Apache  
 $ sudo ufw reload

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

$ sudo systemctl restart apache2.service

* Như vậy là Nagios đã được triển khai và có một giao diện quản lý dưới dạng một website, mặc định sẽ là tại 127.0.0.1/nagios

1. **Thực nghiệm giám sát mạng với Nagios.**
   1. Các dịch vụ giám sát

Để tuỳ biến một dịch vụ giám sát, đầu tiên ta cần định nghĩa lệnh thực thi của dịch vụ đó trong file commands.cfg. Ở đây em định nghĩa thêm 4 lệnh là kiểm tra RAM của máy, kiểm tra các cảm biến nhiệt độ của máy và tuỳ biến 2 lệnh thien\_cmd, thien\_cmd2 dùng để thực thi hai file python để in ra thông số hệ thống.

A screenshot of a cell phone

Description automatically generated

File python thien\_cmd dùng để in ra thông số cấu hình hiện tại của hệ thống

A screenshot of a cell phone

Description automatically generated

Sau khi định nghĩa xong các lệnh thực thi, cần định nghĩa các dịch vụ để hệ thống thực thi. Ở đây em sẽ định nghĩa 4 dịch vụ, các dịch vụ này sẽ sử dụng các lệnh tương ứng vừa định nghĩa ở trên để giám sát máy cá nhân, theo dõi RAM, nhiệt độ, cũng như các thông số hệ thống.

A screenshot of a computer

Description automatically generated

Sau khi thiết lập xong, cần khởi động lại hệ thống Nagios để các thay đổi được áp dụng.

sudo systemctl restart nagios

sudo systemctl status nagios

Hệ thống sẽ hiện thị lên. Nếu các thiết lập chính xác thì hệ thống sẽ hiển thị ở trạng thái active (running), còn không thì sẽ báo lỗi thiết lập.

A close up of text on a black surface

Description automatically generated

* 1. Đánh giá hệ thống và kết quả đạt được

Sau khi thiết lập và khởi động lại hệ thống Nagios, ta kiểm tra lại kết quả thu được tại địa chỉ localhost/nagios. Truy cập vào danh mục các host và lựa chọn host localhost, ta sẽ thấy kết quả của các dịch vụ đang được thiết lập chạy cho localhost

A screenshot of a social media post

Description automatically generated

Các dịch vụ chạy ổn định thì sẽ có trạng thái OK, trong trường hợp khác thì sẽ có những thông báo lỗi tương ứng như WARNING, UNKNOW, CRITICAL.

Lựa chọn 1 dịch vụ và xem thông báo chi tiết của dịch vụ đó. Ở đây ta thử kiểm tra dịch vụ kiểm tra các cảm biến nhiệt độ trên máy. Dịch vụ hoạt động bình thường và trả về thông số là nhiệt độ các cảm biến trên máy nếu có.

A screenshot of a cell phone

Description automatically generated

Với một dịch vụ bị lỗi thì ta cần kiểm tra lại các lệnh commands và thông số cấu hình của dịch vụ, tuỳ vào kết quả báo lỗi của hệ thống.

Ví dụ như dịch vụ thực thi file python thien\_cmd2.py bị lỗi, thì sẽ trả về thông báo lỗi của hệ thống khi thực thi file python này. Còn file python thien\_cmd.py hoạt động ổn định và trả về kết quả đúng như mong đợi.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated