

Học Viện Công Nghệ Bưu Chính Viễn Thông

------------------------------

Sinh viên: Nguyễn Quang Tuấn Lộc

Lớp: An toàn thông tin D14CQAT01-N

MSV: N14DCAT097

BÁO CÁO CHUYÊN ĐỀ AN TOÀN MẠNG

Giám sát thay đổi nội dung thư mục trên máy agent từ xa bằng phần mềm Nagios

**- Yêu cầu thực hành**: Xây dựng và cài đặt máy chủ nagios giám sát sự thay đổi về tên hoặc nội dung của file/folder trên máy Agent

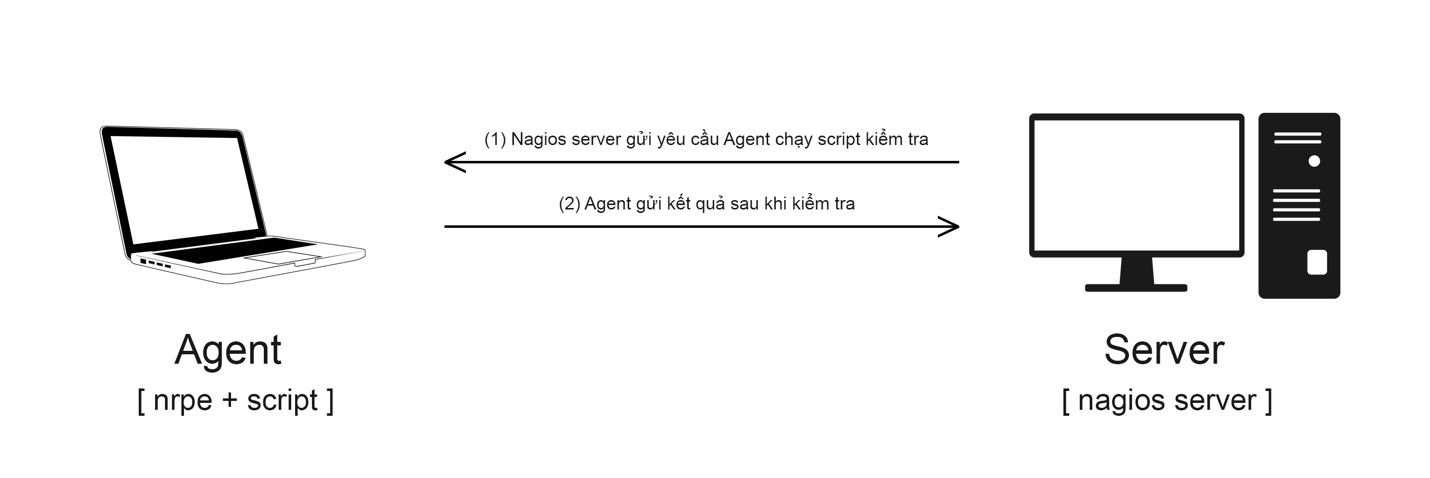
**- Chuẩn bị:**

Ở đây ta dựng Server và Agent trên 2 máy ảo Ubuntu.

Máy Server có ip 192.168.230.128 và máy Agent có ip 192.168.230.136.

# Chương I: Mục Tiêu

Theo dõi sự thay đổi cây thư mục bất kỳ của máy client. Bao gồm: Thêm file mới, xóa file mới, thay đổi nội dung files, thay đổi tên file.



Hình 1.1: Kịch bản giám sát

* Nagios Server:
* OS: Ubuntu 16.04.

Server định kỳ mỗi n phút gửi yêu cầu kiểm tra tới máy client, yêu cầu run file kiểm tra folder đã cài sẵn trên máy client. Sau khi gửi yêu cầu, server sẽ chờ đợi kết quả trả về để hiển thị cho tới khi nhận được kết quả hoặc bắt đầu chu kỳ kiểm tra mới.

* Máy client(agent):

+ OS Ubuntu 16.04.

Khi nhận được yêu cầu từ nagios-server, máy client (agent) sẽ tiến hành thực thi script kiểm tra kiểm tra sự thay đổi, kết quả sẽ được gửi về server ngay sau khi kiểm tra.

**Chương II: Giới thiệu Nagios**

* Nagios là một hệ thống giám sát hạ tầng mạng và dịch vụ mạng vô cùng mạnh mẽ cho phép các doanh nghiệp, công ty xác định và giải quyết các vấn đề về cơ sở hạ tầng Công Nghệ Thông Tin trước khi chúng làm ảnh hưởng đến các hoạt động kinh doanh, vận hành nội bộ của công ty.
* Nagio là một ứng dụng phần mềm miễn phí và mã nguồn mở giám sát hệ thống, mạng và cơ sở hạ tầng. Hiện tại nhà phát triển chỉ hỗ trợ triển khai Nagios hệ thống trên Hệ Điều Hành Linux. Với Nagios bạn sẽ có thêm kênh giám sát và cảnh báo cho các máy chủ, switch, ứng dụng và dịch vụ.
* Các dịch vụ mà Nagios cung cấp
  + Quản lý dịch vụ mạng
  + Giám sát tài nguyên máy chủ
  + Giám sát phần cứng
  + Giám sát từ xa
* Nagios Agent
  + NRPE – Nagios remote plugin excuter
  + NRDP – Nagios remote data processor
  + NCS Client++ (use to monitor windows)
  + NCPA – Nagios cross platform agent
* Chức năng của Nagios
  + Monitoring – giám sát
  + Response – phản hồi
  + Reporting – báo cáo
  + Maintaining – bảo trì bảo dưỡng
  + Planing – lên kế hoạch

**Chương III: Thực hiện giám sát**

Cài đặt Network sử dụng NAT cho cả 2 máy server và agent để tránh ip bị thay đổi khi thay đổi mạng

Để thực hiện việc giám sát ta cần thực hiện qua các bước sau

**B1: Cài đặt và cấu hình Nagios trên server**

* Trước khi cài ta nên cập nhật danh sách các gói cài đặt cho apt-get bằng lệnh:

sudo apt-get update

* Trước tiên ta cài Apache, các gói PHP, các gói openssl, openssh bằng lệnh:

sudo apt update

sudo apt install apache2

sudo apt install php php-cgi libapache2-mod-php php-common php-pear php-mbstring

sudo apt-get install openssl

sudo apt-get install libssl-dev

sudo apt-get install openssh-server openssh-client

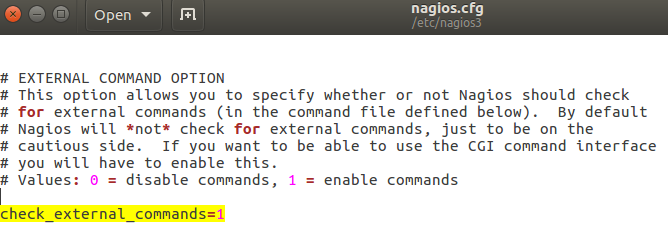
* Tiến hành cài nagios

sudo apt install nagios3 nagios-plugins-basic

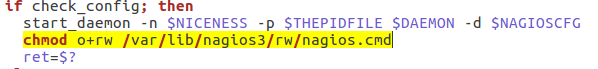
trong quá trình cài đặt sẽ hiện thông báo tạo password cho nagiosadmin

* Cấu hình nagios trên máy server:

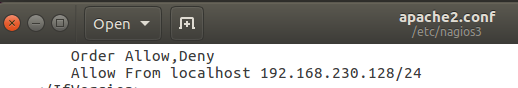
sudo gedit /etc/nagios3/nagios.cfg



sudo gedit /etc/init.d/nagios3



sudo gedit /etc/nagios3/apache2.conf

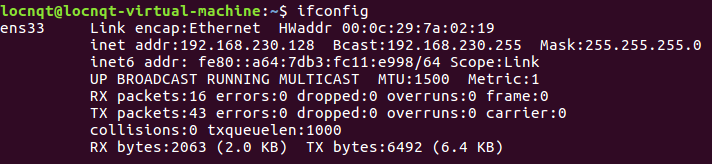


sudo chgrp -R www-data /var/lib/nagios3

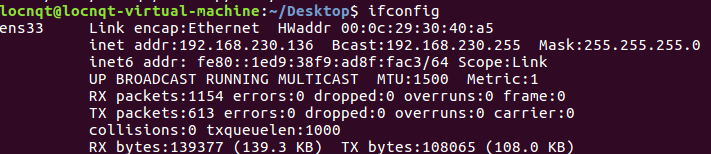
sudo chmod 750 /var/lib/nagios3/rw

sudo systemctl restart nagios3.service

sudo systemctl restart apache2.service

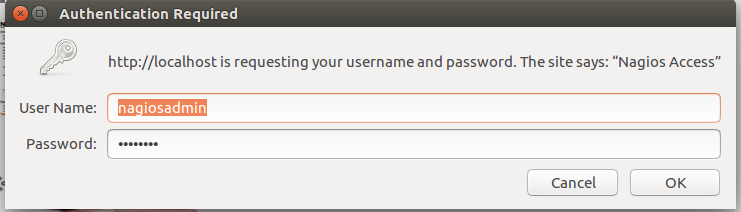


Server có ip: **192.168.230.128**



Agent có ip: **192.168.230.136**

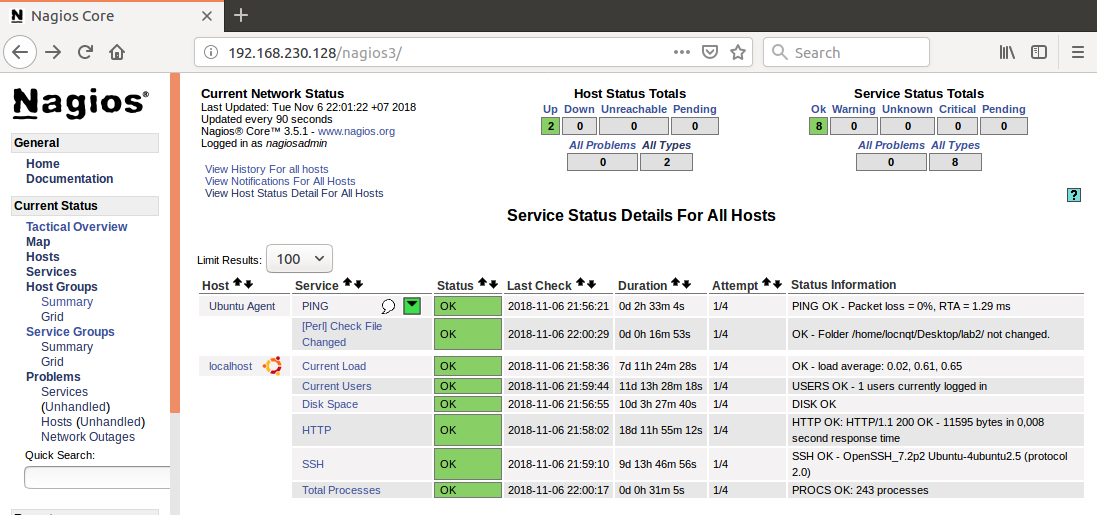
* Mở browser truy cập tới **http://localhost/nagios3** hoặc **http://192.168.230.128/nagios3/** truy cập vào giao diện web của Nagios bằng tài khoản nagiosadmin và password đã tạo.





Giao diện của Nagios

* Click vào Services



**B2: Xây dựng Perl Script**

* Script này sẽ chạy trên máy Agent.
* Để chạy đươc perl script ta phải cài perl và các thư viện cần thiết:

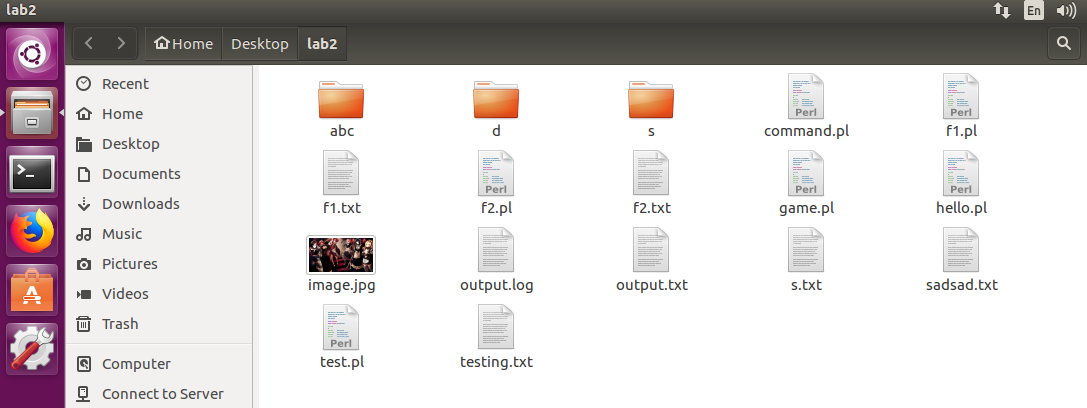
sudo cpan

cpan[1]> upgrade

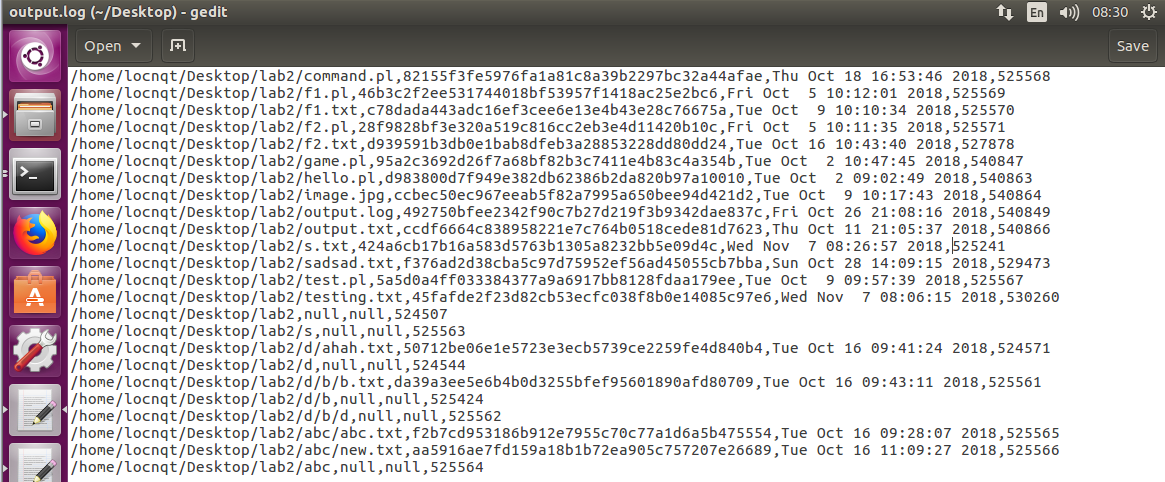
sudo apt-get install cpanm

cpanm -i Digest::SHA1

* Ý tưởng: ta sẽ dùng hàm băm(SHA1) để kiểm tra sự thay đổi về nội dung và dùng id để kiểm tra tên, đường dẫn để kiểm tra vị trí file
* Ta sẽ theo dõi folder lab2 có path là /home/locnqt/Desktop/lab2/



* File output.log để ghi lại các trạng thái cần theo dõi:

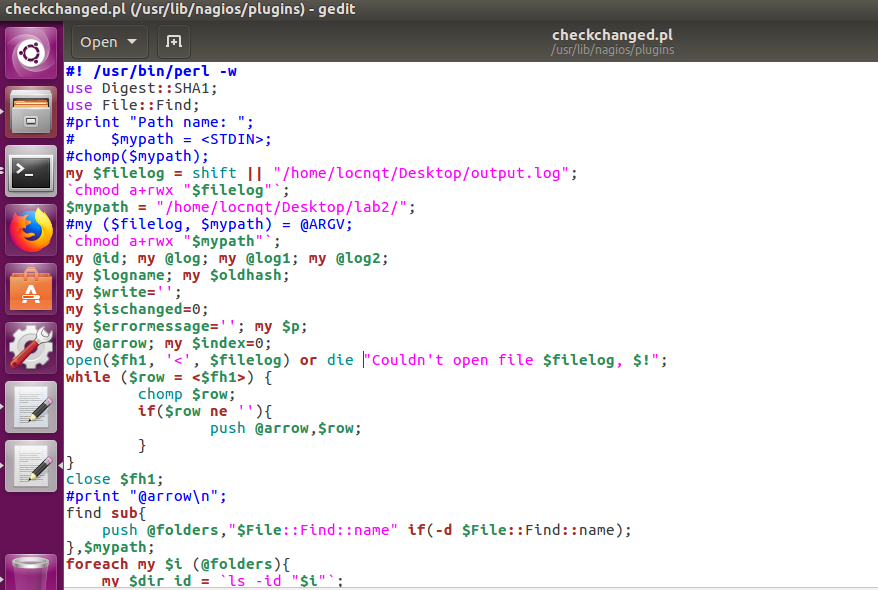


Ta sẽ lưu ở đây: đường dẫn đến file cần theo dõi, mã băm của file đó, ngày cập nhật của file đó và id của file. Đối với folder thì ta cho mã băm và ngày cập nhật bằng null.

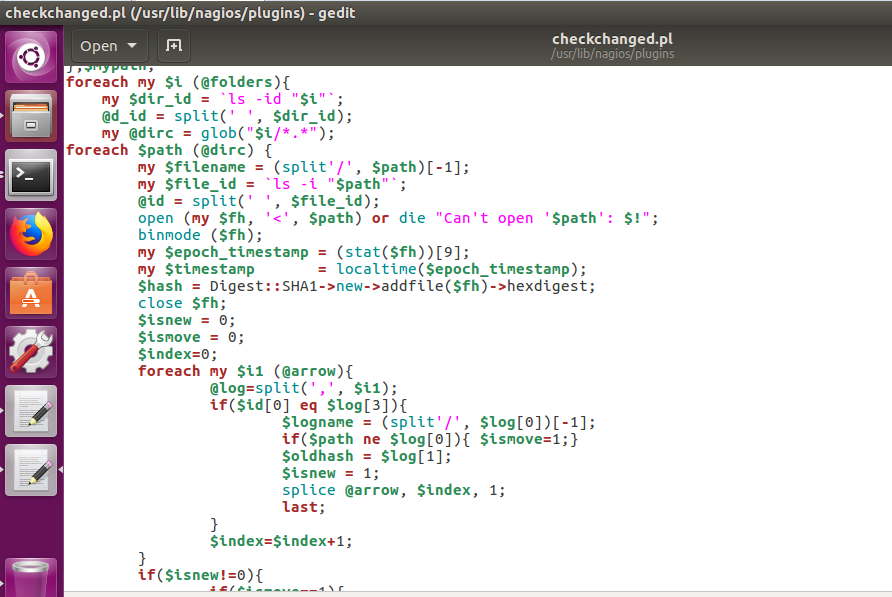
* Ta cấp quyền cho script bằng lệnh:

sudo chmod +x /usr/lib/nagios/plugins/checkchanged.pl

* Nội dung script:



Đầu tiên ta mở file log và ghi từng dòng trong file log vào mảng @arrow. Sau đó ta tìm tất cả các thư mục và lưu hết vào mảng @folders.



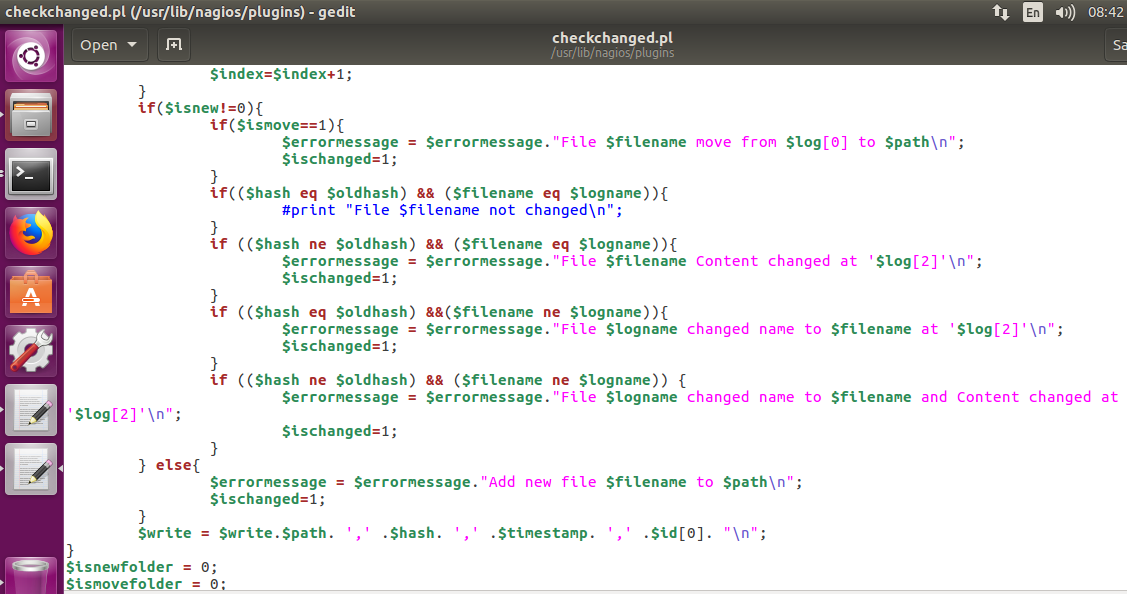
Duyệt từng thư mục có trong mảng @folders.

Duyệt từng file có trong thư mục đang được duyệt:

Ta lưu tên file vào biến $filename, dùng lệnh ls –i để lấy id của file đang duyệt và lưu vào biến $id[0].

Dùng SHA1 để băm file và lưu mã băm được vào biến $hash. Dùng biến $timestamp lưu thời gian thay đổi file.

Duyệt trong mảng @arrow và tiến hành tìm id trùng với id file đang duyệt: tại đây ta lấy các thông tin của file đó thông qua id đã lưu trên file log. Sau đó xóa dòng đó ra khỏi mảng @arrow



Với các file đang duyệt sẽ kiểm tra các trường hợp sau:

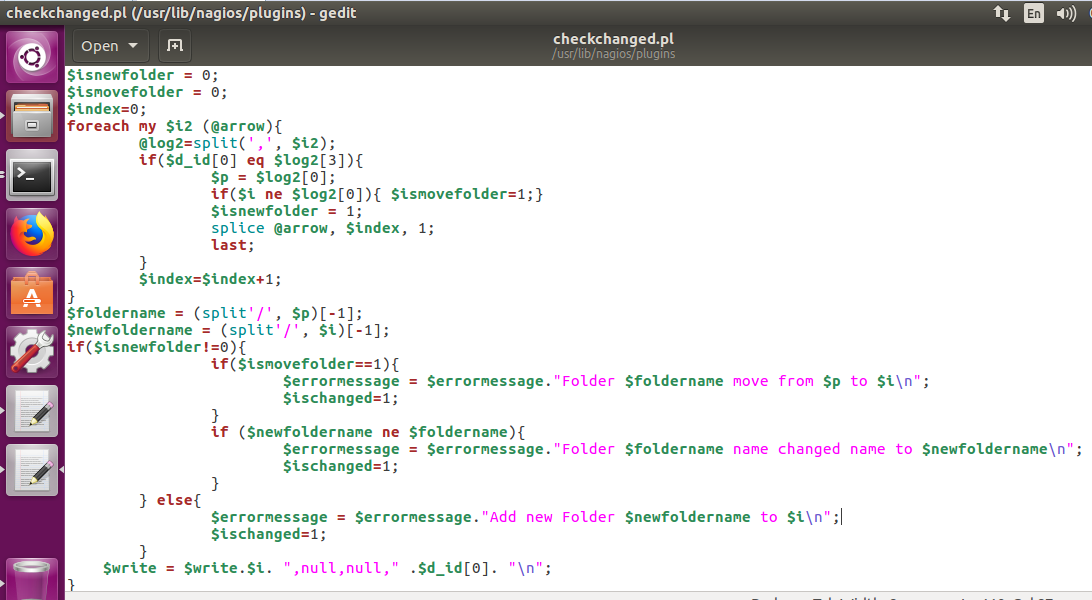
+Là file mới: ta dùng biến $isnew để kiểm tra. Nếu bằng 0 thì là file mới còn bằng 1 thì là không phải là file mới. Biến sẽ bật lên 1 khi tìm thấy id file trong file log.

+File bị di chuyển(nhưng vẫn nằm trong thư mục lab2): dùng biến $ismove để kiểm tra. Nếu bằng 1 thì file đã chuyển qua thư mục khác còn nếu bằng 0 thì vẫn không thay đổi. Biến sẽ bật lên 1 khi so sánh đường dẫn file đang duyệt với đường dẫn lấy từ file log không bằng nhau.

+Nội dung file thay đổi: ta sẽ so sánh mã băm của file với mã băm lưu trong file log

+Đổi tên: kết hợp giữa so sánh id, mã băm, đường dẫn.

Sau khi kiểm tra ta lưu lại tất cả thông tin mới của file vào biến $write



Với các folder đang duyệt sẽ kiểm tra các trường hợp sau:

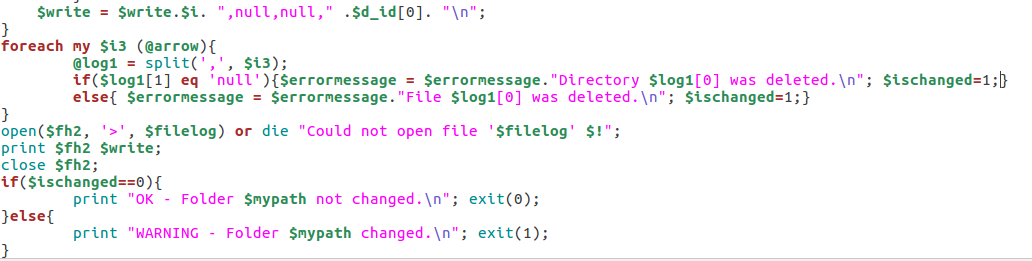
+Kiểm tra folder mới: ta dùng biến $isnewfolder để kiểm tra. Nếu bằng 0 thì là folder mới còn bằng 1 thì là không phải là folder mới. Biến sẽ bật lên 1 khi tìm thấy id folder trong file log.

+Kiểm tra folder bị đổi tên: so sánh tên id folder đang duyệt có trong file log không. Nếu có thì so sánh tên có bị đổi không.

+Kiểm tra folder bị dịch chuyển qua thư mục khác: dùng biến $ismovefolder để kiểm tra. Nếu bằng 1 thì folder đã chuyển qua thư mục khác còn nếu bằng 0 thì vẫn không thay đổi. Biến sẽ bật lên 1 khi so sánh đường dẫn folder đang duyệt với đường dẫn lấy từ file log không bằng nhau.

+Kiểm tra nội dung folder: do folder có nội dung là folder phải có file và ta đa duyệt ở trên rồi nên không làm lại

Sau khi kiểm tra ta lưu lại tất cả thông tin mới của folder vào biến $write



-Kiểm tra xóa: ta duyệt mảng @arrow. Do trong quá trình quét thư mục ở trên ta có lệnh xóa dòng thông tin của file/folder được tìm thấy nên những gì còn lại trong file log sẽ là của các file/folder đã bị xóa(nên không tìm thấy trong quá trình duyệt).

Ta ghi mới biến $write vào file log để cập nhật lại file log.

Cuối cùng là xuất thông báo và trạng thái dựa trên biến $ischanged. Biến $ischanged sẽ bằng 1 nếu có bất kỳ thay đổi nào trong các lần kiểm tra.

**B3: Cài đặt và cấu hình NRPE**

**+ AGENT SIDE:**

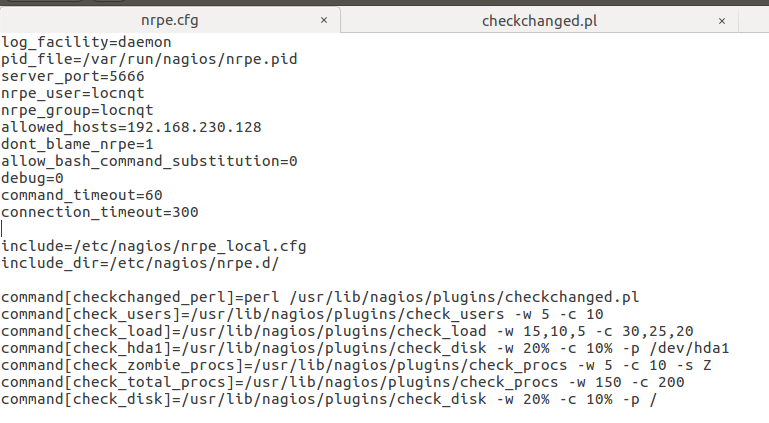
* Cài openssl, openssh.
* Cài đặt NRPE và trình biên dịch Perl trên Agent





* Tiến hành cấu hình NRPE





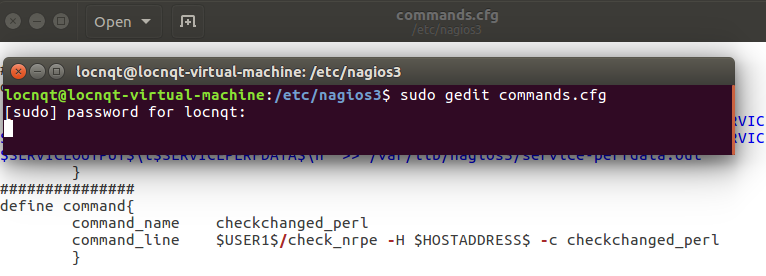
* Allowed\_hots = 192.168.230.128 (IP Nagios Server)
* Định nghĩa command là **checkchanged\_perl**. Mục đích là khi Nagios server gọi command này sẽ tương đương với vế bên phải, tức là sẽ thực thi câu lệnh

**perl /usr/lib/nagios/plugins/checkchanged.pl**= thực thi script checkchanged.pl trên máy Agent và trả kết quả về cho Nagios

* Khởi động lại NRPE: **sudo /etc/init.d/nagios-nrpe-server restart** và **sudo systemctl restart nagios-nrpe-server**

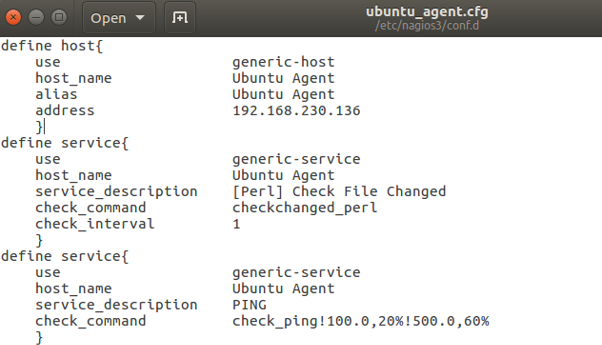
**+ SERVER SIDE**

* Cài đặt: sudo apt-get -y install nagios-nrpe-plugin
* Định nghĩa command trong file command.cfg



* Định nghĩa command với tên giống như cấu hình bên phía Agent là **checkchanged\_perl** như trong hình và lưu lại
* Định nghĩa Service cho command này



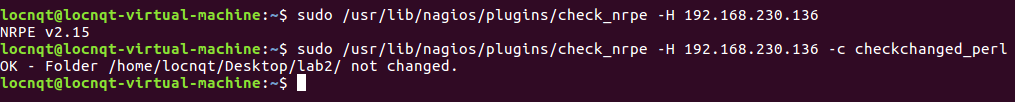


* Ta quan tâm tới các thuộc tính **host\_name** – tên máy Agent, **address** địa chỉ ip của Agent(192.168.230.136), **check\_commnd** – tên command được gọi, **check\_interval** – thời gian mỗi lần kiểm tra (1 tức là 1phút) mỗi phút thì Nagios sẽ gọi command này 1 lần để kiểm tra. Ta có thể thêm service PING để kiểm tra ping giữa server với agent.
* Sau khi hoàn tất việc cấu hình ta restart lại dịch vụ bằng lệnh:

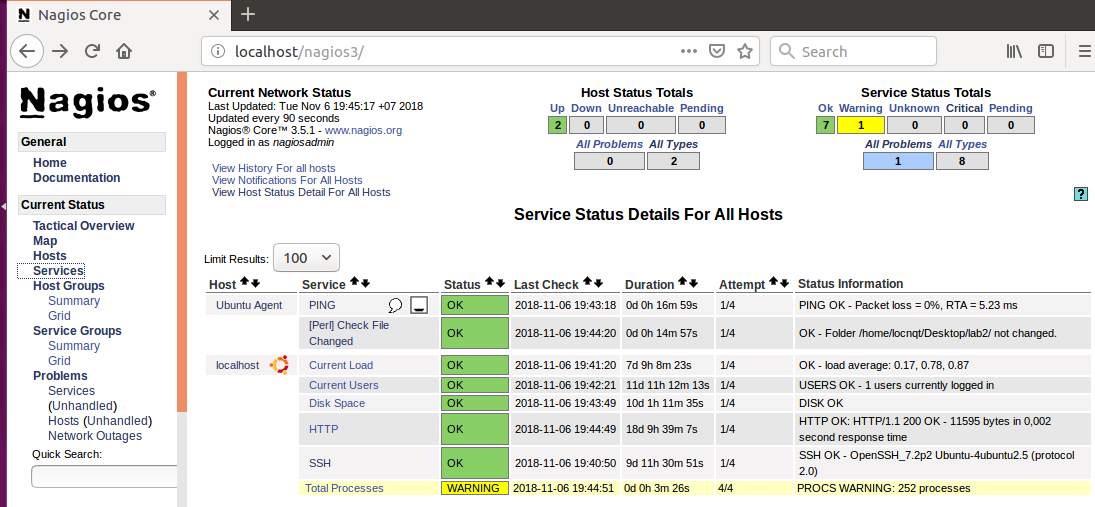
sudo systemctl restart nagios3

**B4: Tích hợp script vào plugin**

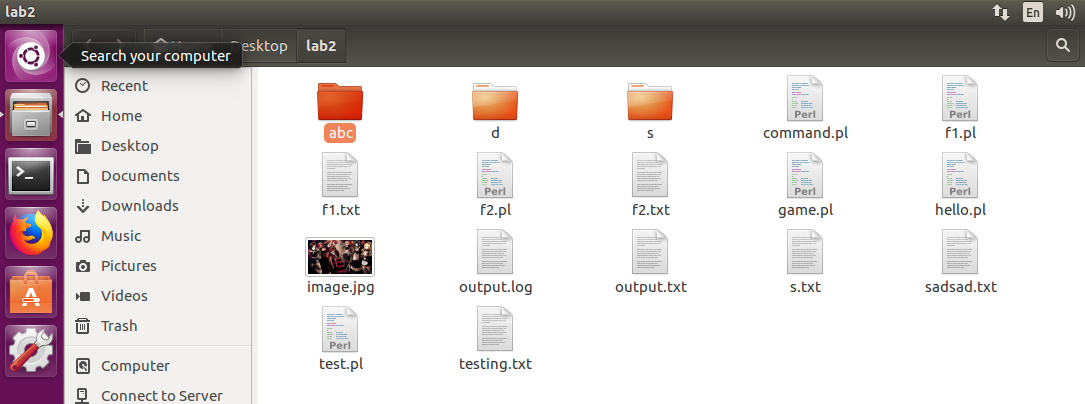
* Ta lưu **checkchanged.pl** vào đường dẫn **/usr/lib/nagios/plugins/** trên máy agent
* Tiến hành kiểm tra xem NRPE đã hoạt động hay chưa

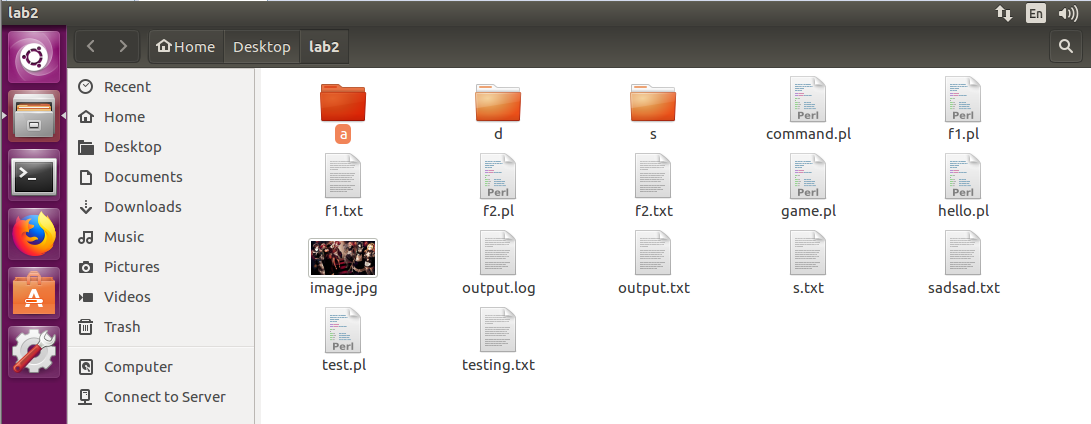


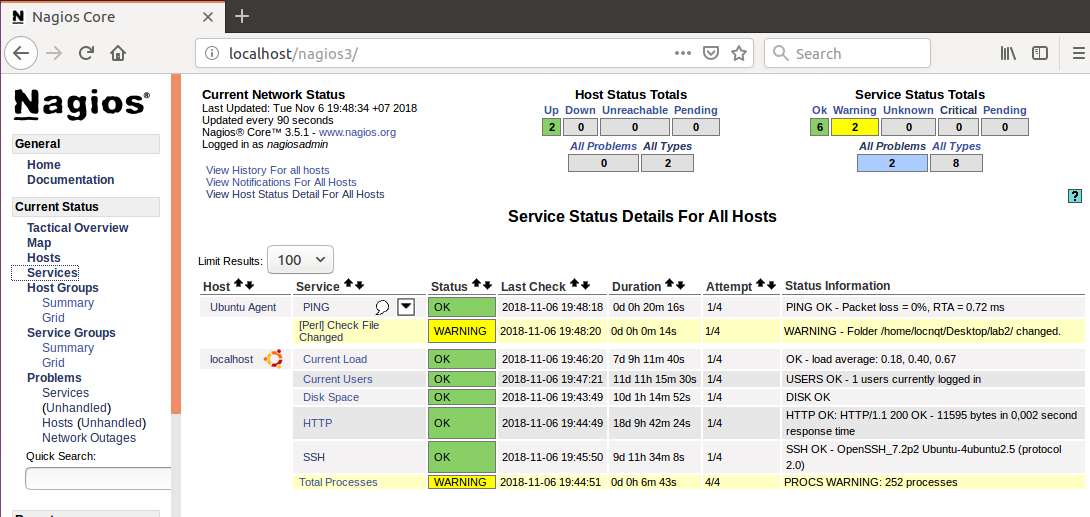
**KẾT QUẢ**



* Tiếp đến ta sẽ thêm mới, thay đổi nội dung hoặc tên của File/Folder ,xóa hoặc di chuyển File/Folder bất kì trong thư mục gốc
* Nagios sẽ phát cảnh báo







* Sau 1 phút sẽ tự động quét lần nữa và không thay đổi gì thì sẽ quay về trạng thái OK

