BÁO CÁO CHUYÊN ĐỀ AN TOÀN MẠNG

Sinh viên: Trần Thanh Bình

Lớp: An toàn thông tin D14

MSV: N14DCAT048

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

**Chương I: Giới thiệu Nagios**

* Nagios là một ứng dụng phần mềm mã nguồn mở hoàn toàn miễn phí có chức năng giám sát hệ thống, mạng và cơ sở hạ tầng
* 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 II: 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

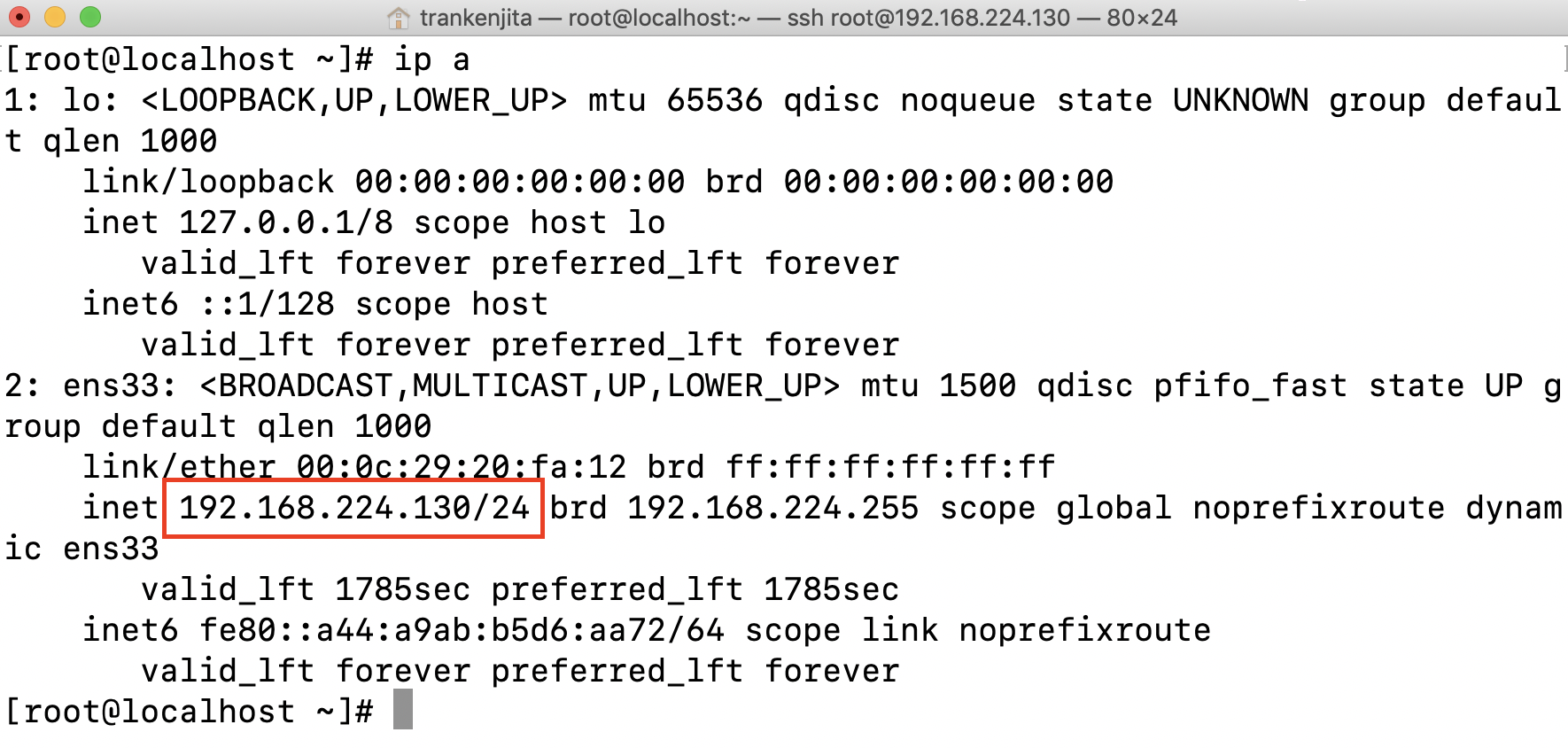
* Để thực hiện việc giám sát ta cần thực hiện qua các bước sau
  + Cài đặt và cấu hình Nagios server trên máy CentOS, tạo kết nối Ubuntu tới Server
  + Tiến hành tải Agent và cài đặt trên máy Ubuntu
  + Xây dựng perl script kiểm tra sự thay đổi về tên hoặc nội dung của file/folder
  + Cài đặt và cấu hình NRPE trên máy Server(CentOS) và máy Agent(Ubuntu)
  + Tích hợp perl script vào plugin trên máy agent

**B1: Cài đặt và cấu hình Nagios**

* Download NagiosXI được tích hợp sẵn trên máy ảo CentOS VMWare tại trang chủ Nagios.com theo địa chỉ: <https://www.nagios.com/downloads/nagios-xi/vmware/>
* Sau khi tải xong, import máy ảo vào VMWare và đăng nhập CentOS với tài khoản mặc định

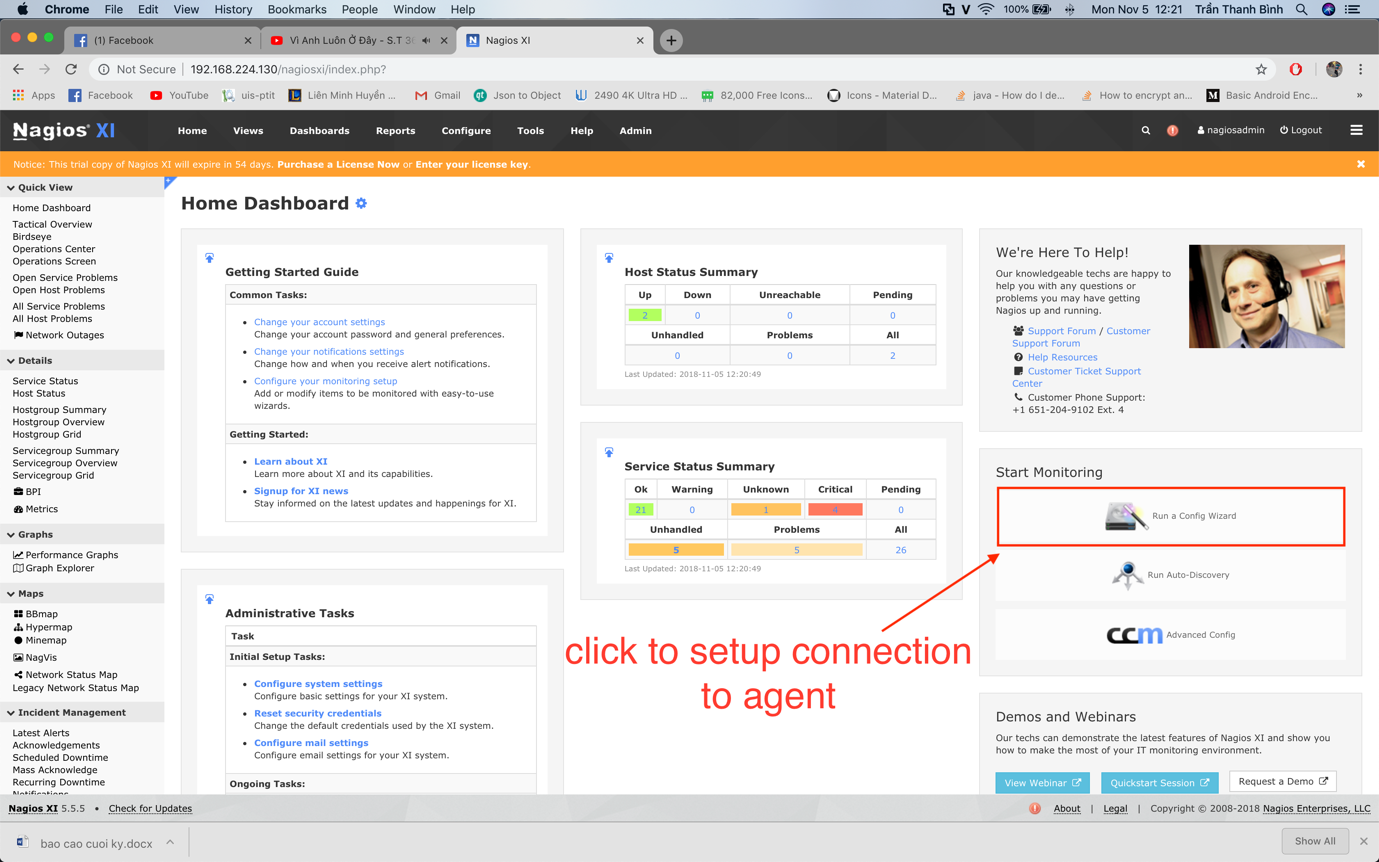
**username/password = root/nagiosxi**

**ip a** – sử dụng để check ip máy server



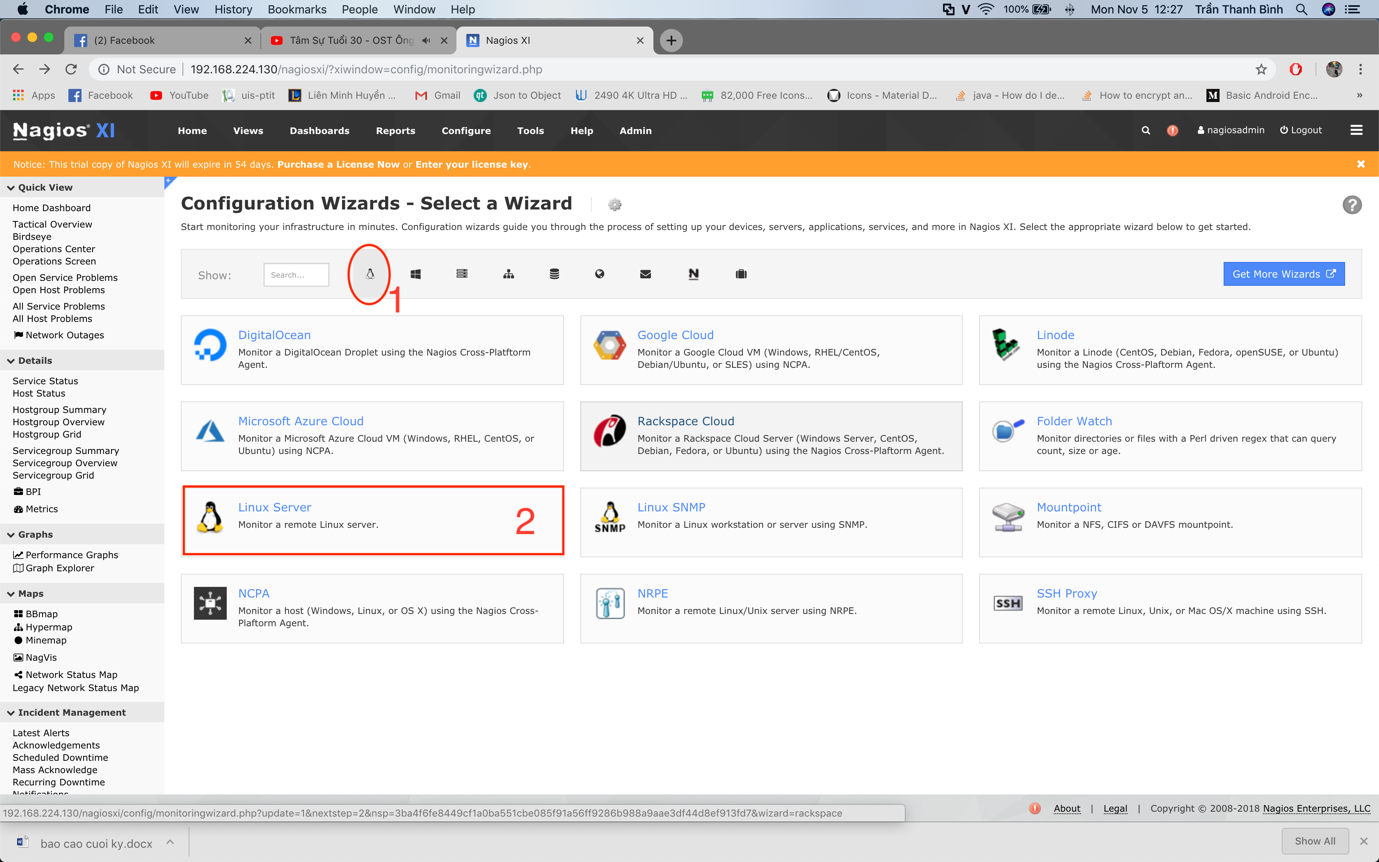
Server có ip: **192.168.224.130**

* Mở browser truy cập tới **192.168.224.130** Access NagiosXI và setup mật khẩu cho tài khoản truy cập, tiến hành hoàn tất cài đặt và truy cập vào giao diện web của NagiosXI

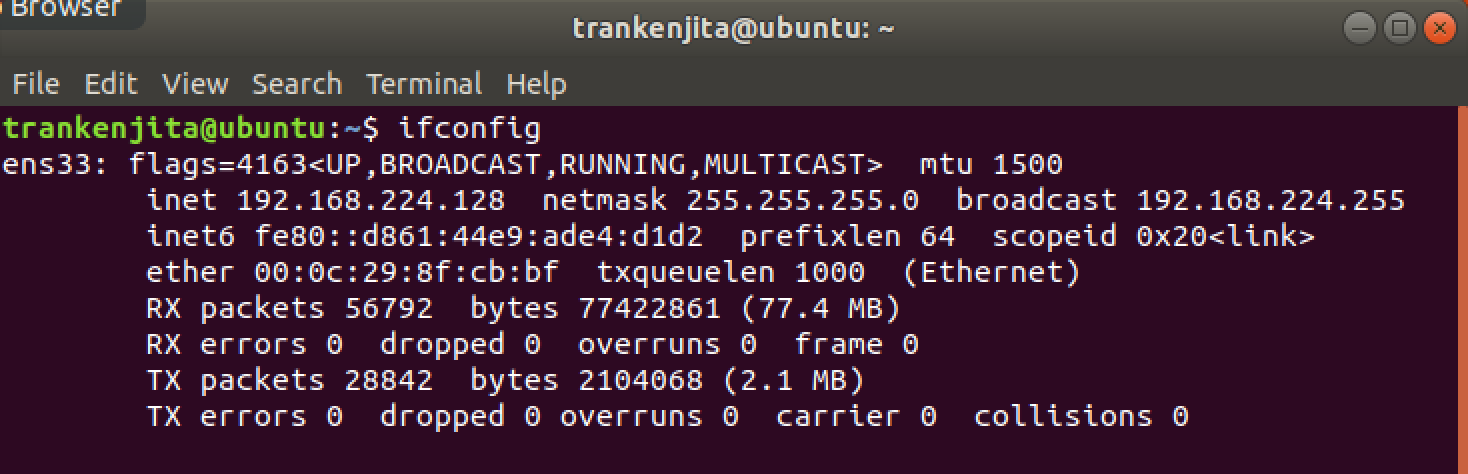
****

Giao diện của NagiosXI

* Sau khi click Config wizard ta chọn phần thiết lập cho Linux Server



* Kiểm tra ip máy agent cần theo dõi (Ubuntu) ta dc ip agent: **192.168.224.128**

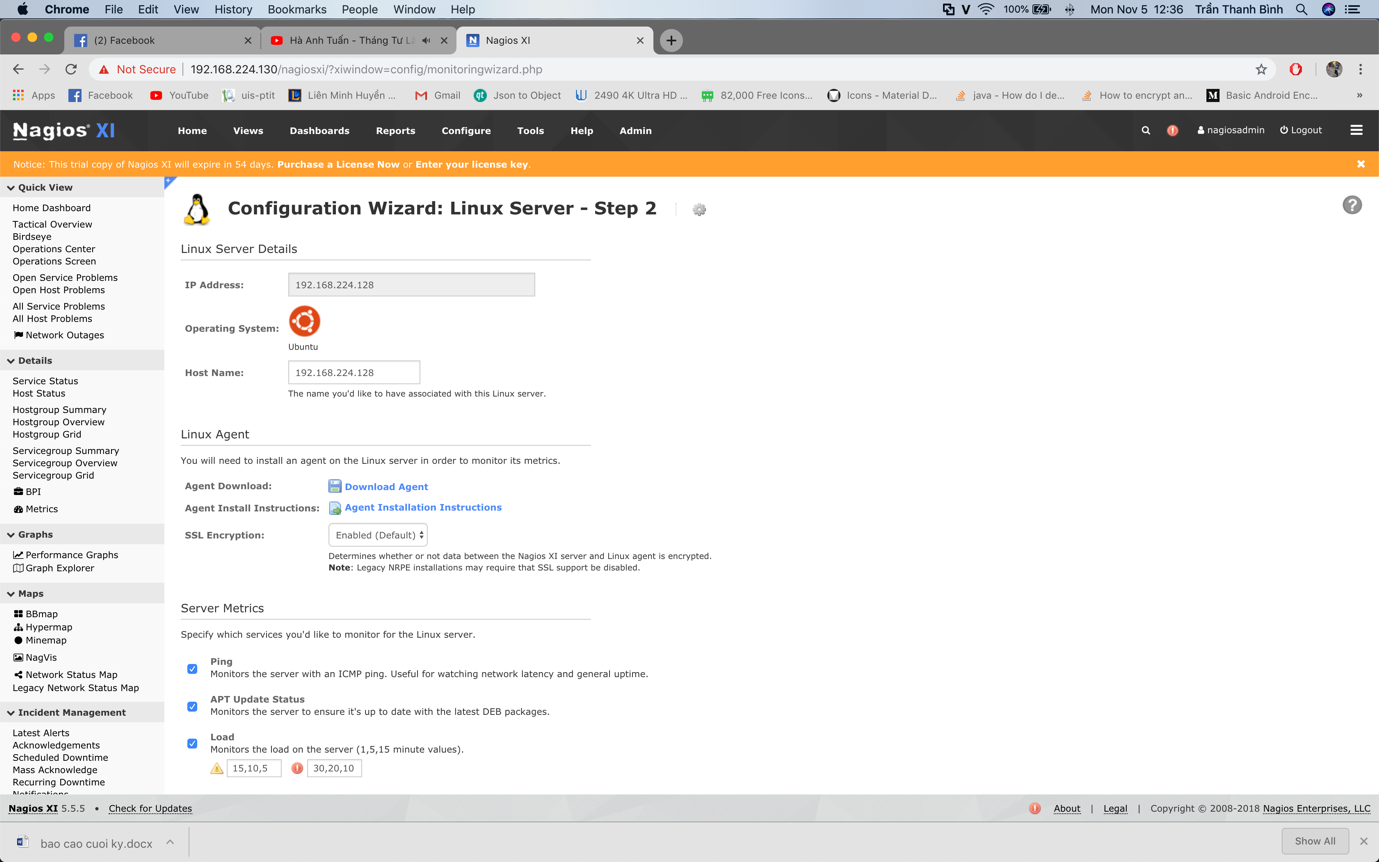




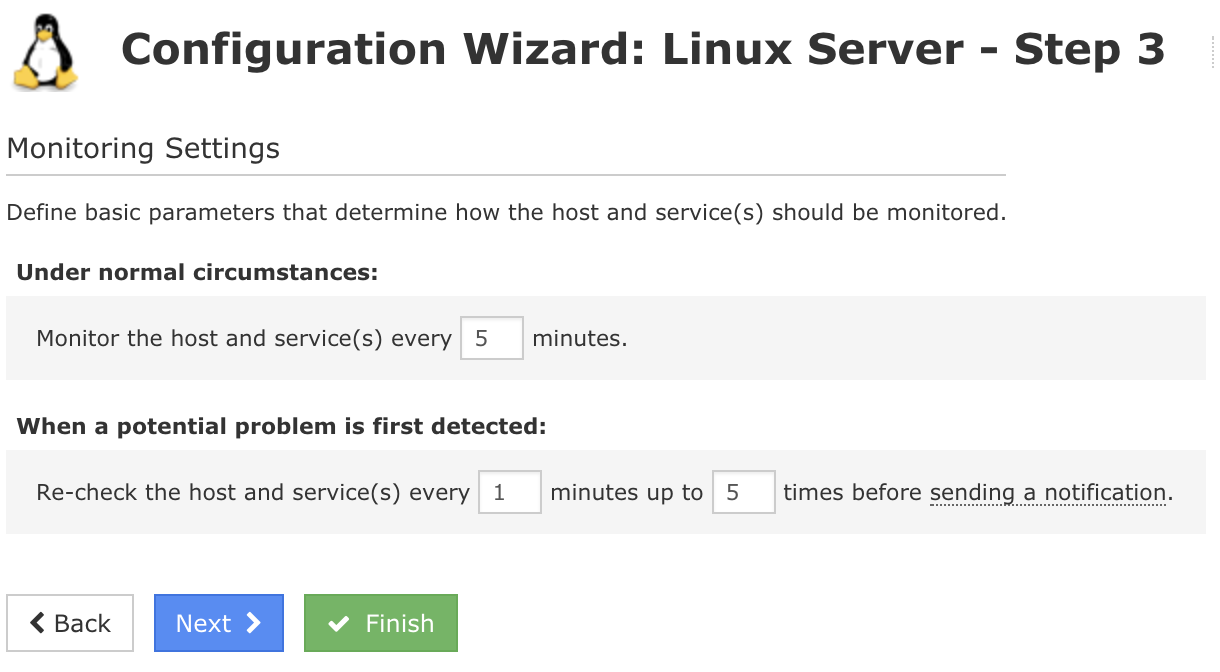
Điền thông tin máy agent cần thiết lập kết nối

**B2: Tiến hành tải Agent về và cài đặt trên máy Ubuntu**

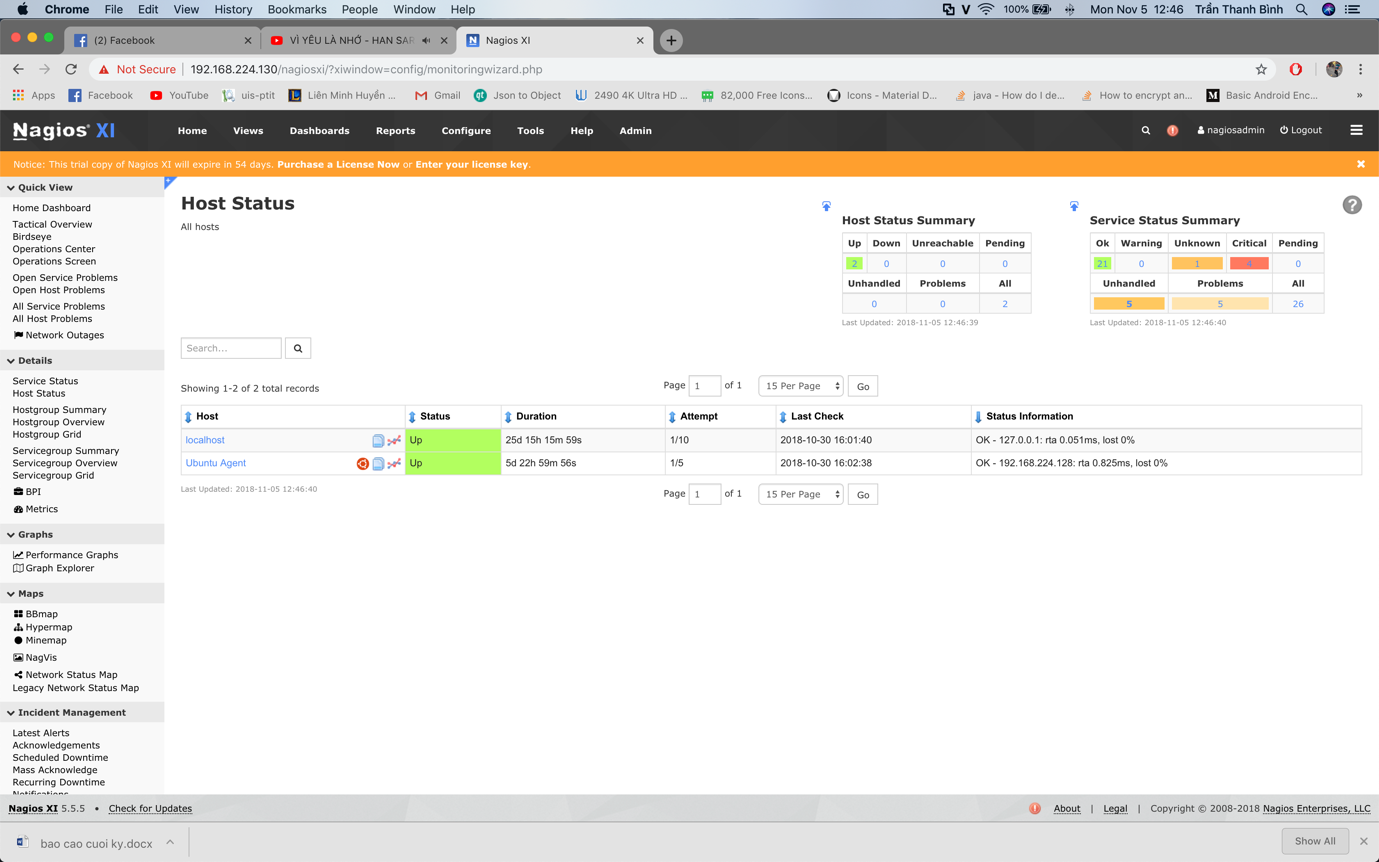
* Sau khi điền xong thông tin máy agent tại B1,click Next để tải NRPE cho Agent



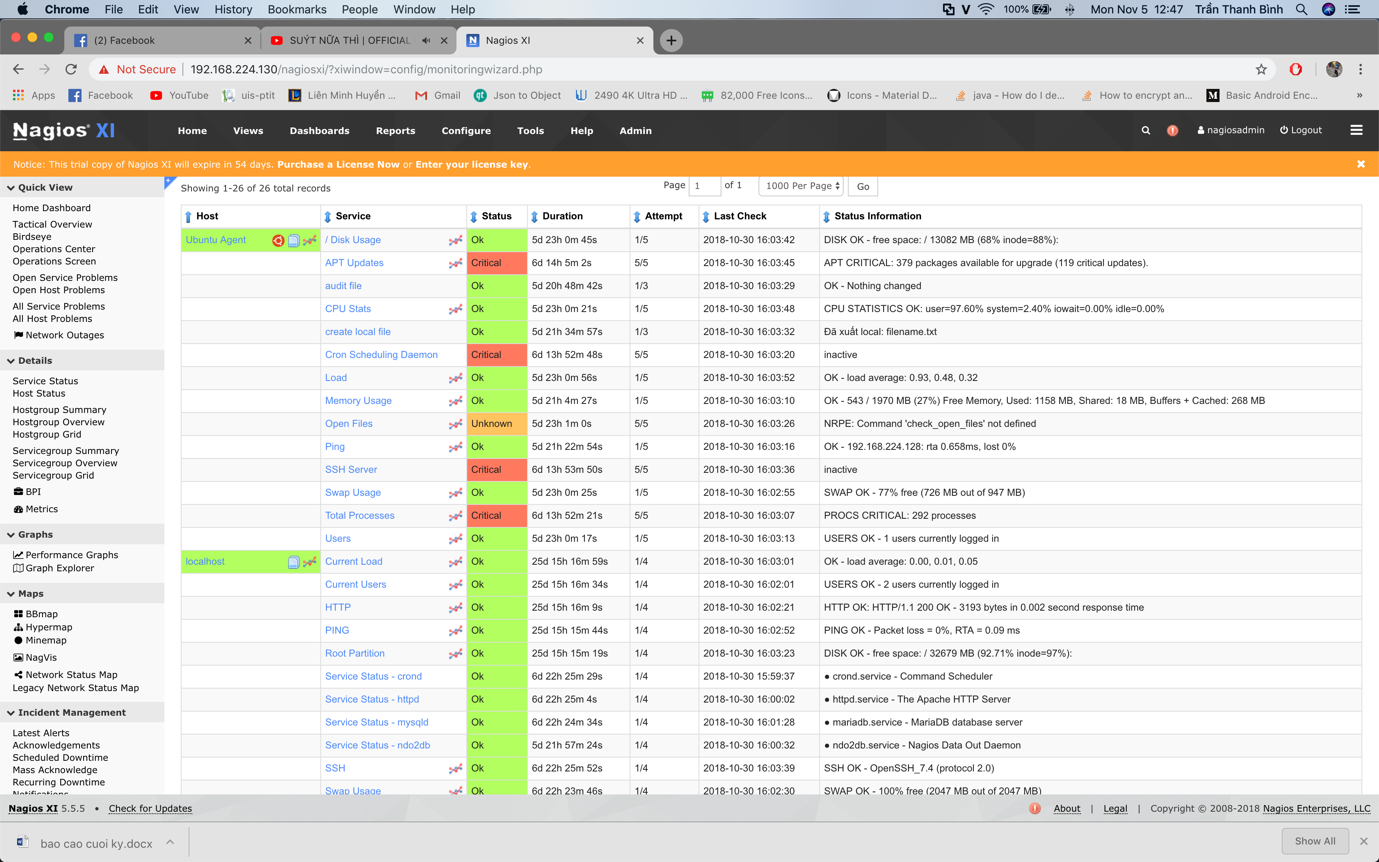
* Kéo xuống dưới cùng, click Next tới màn hình kế tiếp



* + Tiến hành cài đặt giám sát như trên hình: Giám sát host và service mỗi 5 phút sẽ gửi báo cáo về, nếu lần đầu tiên đã phát hiện vấn đề thì sẽ kiểm trả lại host và service mỗi 1 phút 1 lần, kiểm tra tới 5 lần trước khi gửi thông báo
  + Có thể rút ngắn thời gian tùy vào độ quan trọng của dữ liệu
* Sau khi hoàn tất, click Finish để hoàn tất
* Copy file Agent tải về vào máy Ubuntu và tiến hành giải nén và cài đặt. Sau khi hoàn tất cài đặt kiểm tra kết nối trên Nagios xem 2 máy đã kết nối chưa



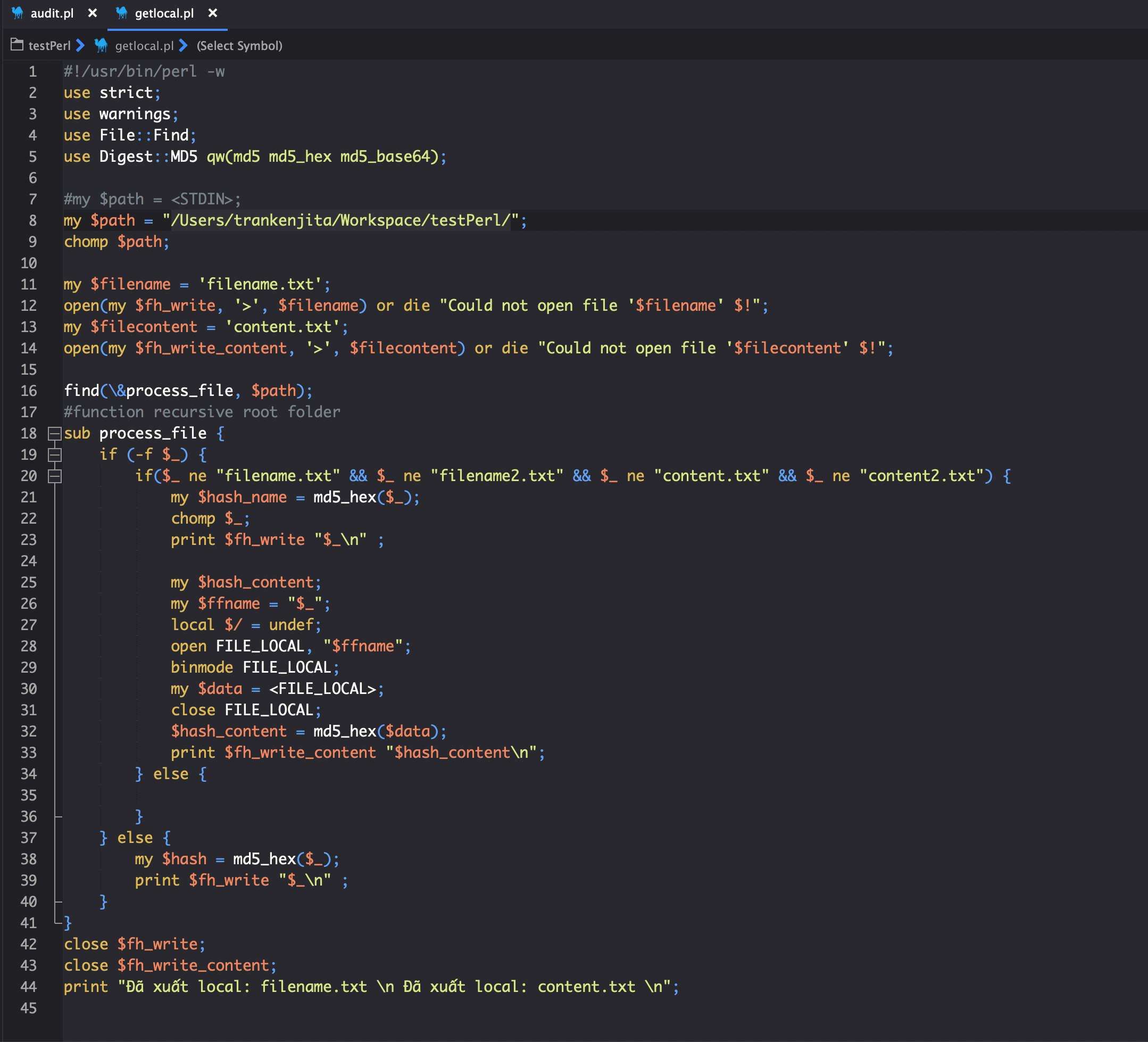
Status UP – tình trạng đã kết nối thành công



Các services đang được theo dõi bởi Nagios trên máy Ubuntu

**B3: Xây dựng Perl Script**

* Ta nhận thấy File sẽ có 2 thành phần là tên và nội dung, còn Folder chỉ có 1 thành phần là tên. Vì thế ý tưởng là sẽ gán nội dung của Folder là rỗng. tức là Folder giờ cũng có 2 thành phần là tên và nội dung (nhưng nội dung = null)
* Xây dựng script để tạo ra file gốc với tên **getlocal.pl**, nhiệm vụ của script này sẽ tạo ra file gốc chứa tên và nội dung chuẩn (lúc chưa bị thay đổi)

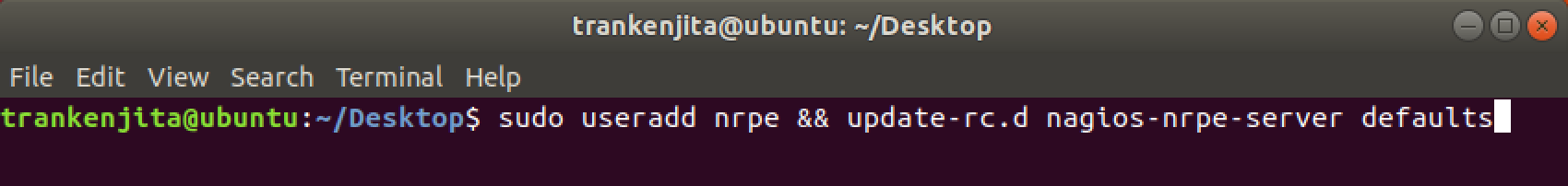


* Sau đó ta gọi đệ quy từ thư mục gốc với đường dẫn cố định truyền vào biến **$path**, hàm đệ quy sẽ quét toàn bộ các File và Folder nằm trong thư mục gốc. Đồng thời ta tạo ra 2 con trỏ với 2 mục đích ghi lại tên và nội dung của File và Folder và ghi lại vào 2 file riêng biệt là **filename.txt** và **content.txt**
* Sau khi đã có thư mục gốc ta xây dựng script thứ 2 với tên **audit.pl**, nhiệm vụ của script này tương tự như **getlocal.pl**, tuy nhiên tên và nội dung sẽ được lưu vào 2 file khác là **filename2.txt và content2.txt**. Sau đó sẽ tiến hành so sánh nội dung của **filename.txt** và **filename2.txt**, **content.txt** và **content2.txt**. Từ đó đưa ra kết quả file/folder đã bị thay đổi tên hoặc nội dung hay chưa

**B4: Cài đặt và cấu hình NRPE**

**+ AGENT SIDE:**

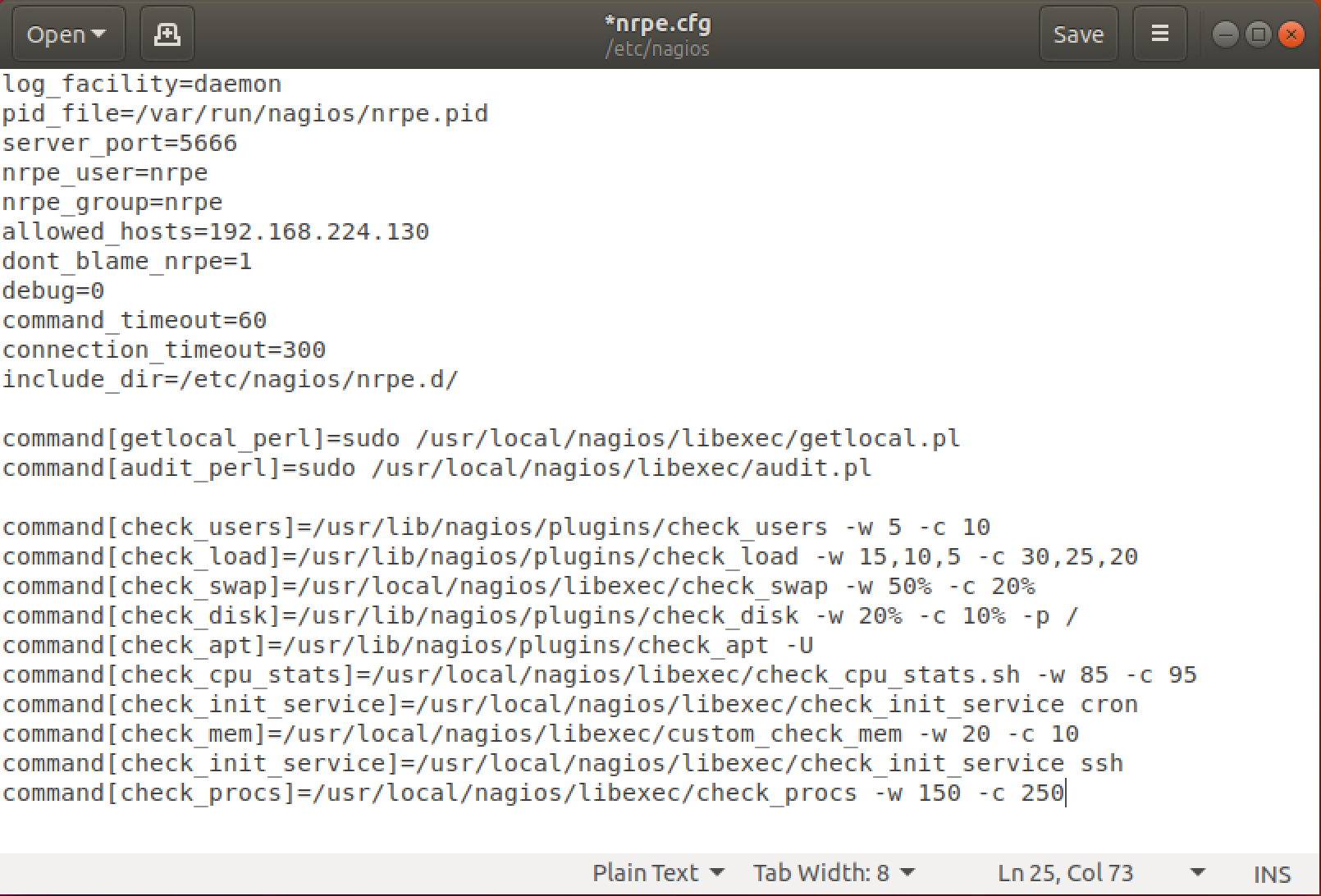
* Cài đặt NRPE và trình biên dịch Perl trên Ubuntu





* Tiến hành cấu hình NRPE





* Allowed\_hots = 192.168.224.130 (IP Nagios Server)
* Định nghĩa 2 command là **getlocal\_perl** và **audit\_perl**. Mục đích là khi Nagios server gọi 2 command này sẽ tương đương với vế bên phải, tức là sẽ thực thi câu lệnh

**Sudo /usr/local/nagios/libexec/getlocal.pl** = thực thi script getlocal.pl trên máy Ubuntu và trả kết quả về cho Nagios

* Thêm ip nagios server vào đây



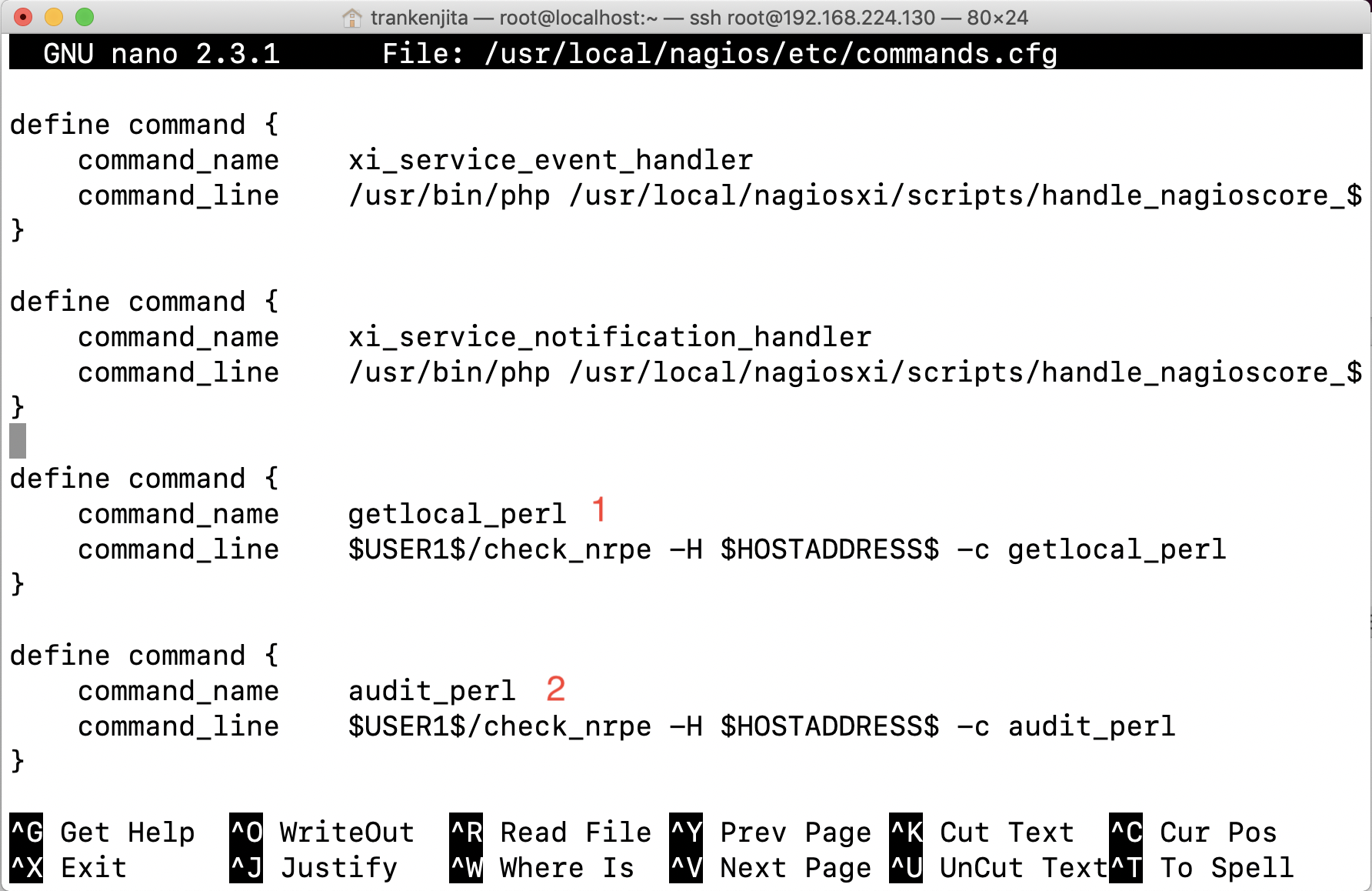


* Khởi động lại NRPE: **services nagios-nrpe-server restart**

**+ SERVER SIDE**

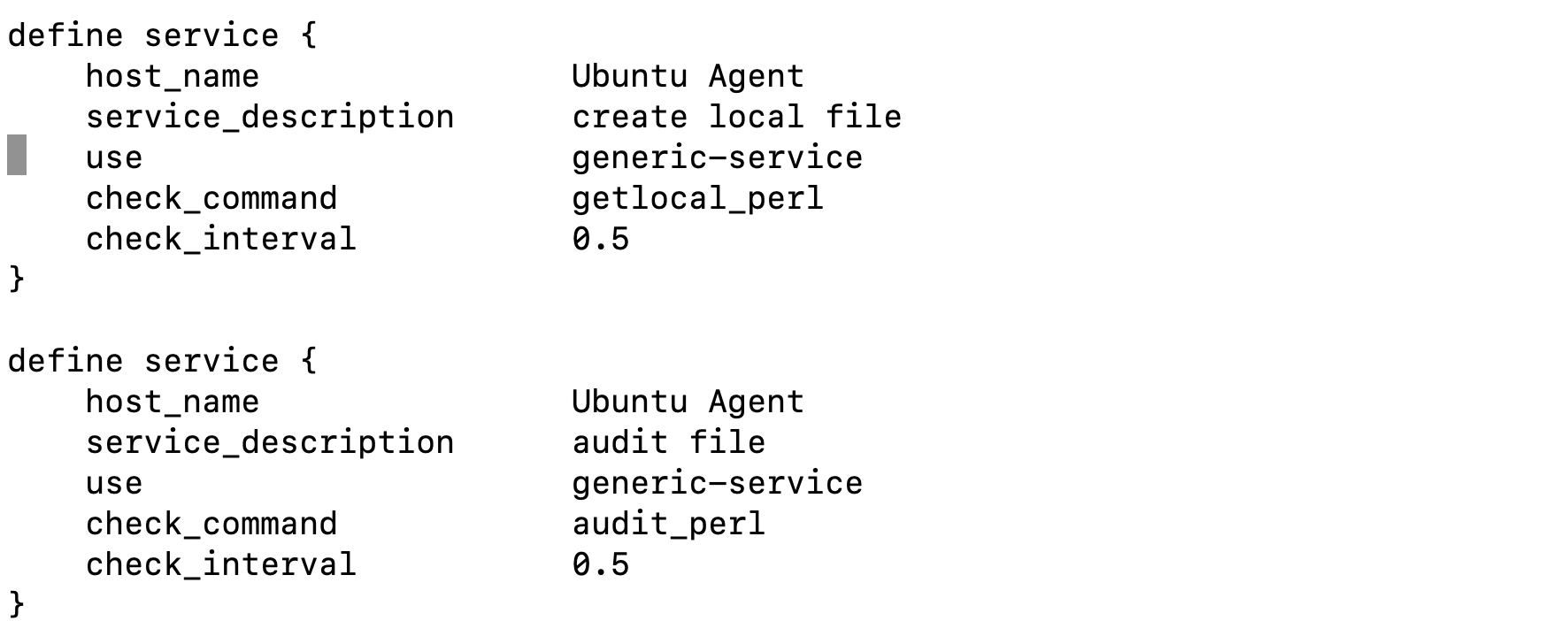
* Định nghĩa command trong file command.cfg



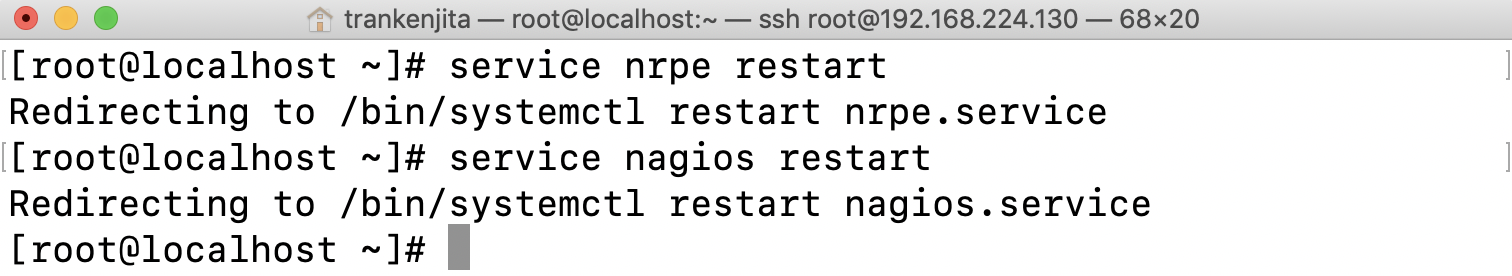


* Định nghĩa 2 command với tên giống như cấu hình bên phía Agent là **getlocal\_perl** và **audit\_perl** như trong hình và lưu lại
* Định nghĩa Service cho 2 command này



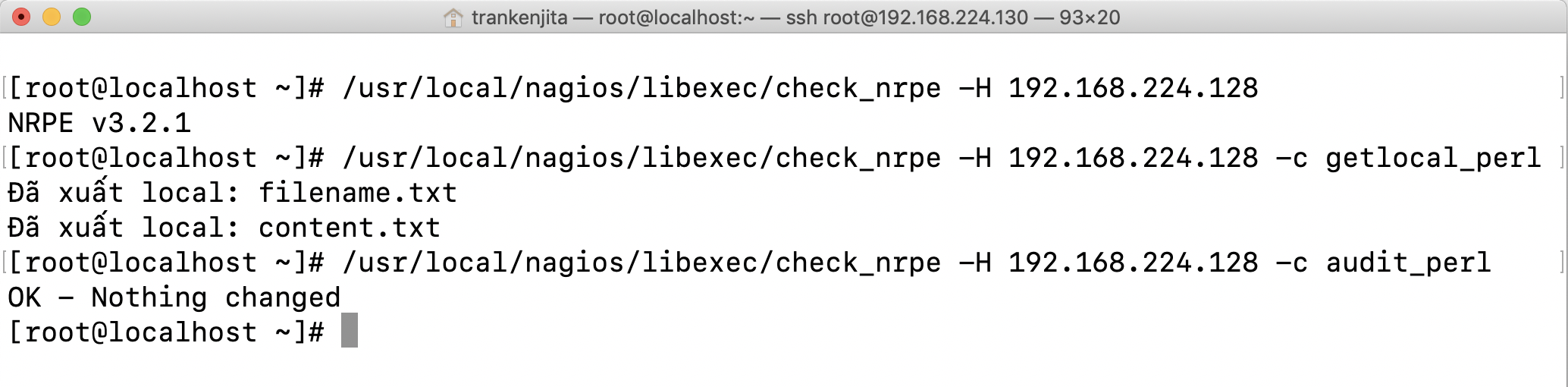


* Ta quan tâm tới các thuộc tính **host\_name** – tên máy Agent, **check\_commnd** – tên command được gọi, **check\_interval** – thời gian mỗi lần kiểm tra (1 = 1m = 60s, đặt 0.5 tương đương với 30s) tức là mỗi 30s thì Nagios sẽ gọi command này 1 lần để kiểm tra
* Sau khi hoàn tất việc cấu hình ta restart lại dịch vụ Nagios và NRPE



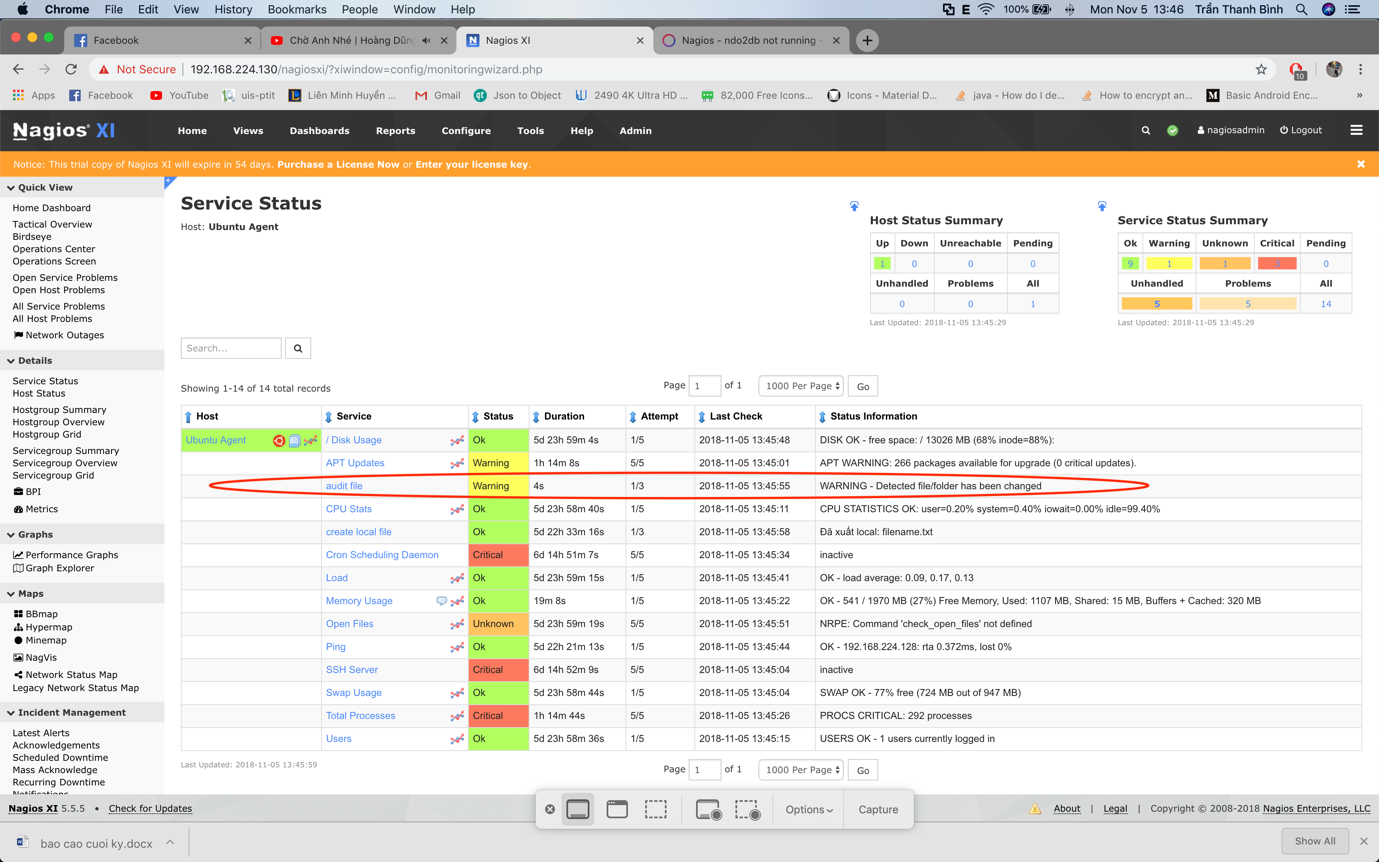
**B5: Tích hợp script vào plugin**

* Copy 2 script **getlocal.pl** và **audit.pl** vào đường dẫn **/usr/local/nagios/libexec** trên máy agent
* Tiến hành kiểm tra xem NRPE đã hoạt động hay chưa



**KẾT QUẢ**

* Ta tạo 1 folder với đường dẫn như trong script, tiến hành tạo các folder con, các file trong mỗi folder
* Sau đó tiến hành gọi script **getlocal.pl** để in ra file gốc
* Tiếp đến ta thay đổi nội dung hoặc tên của File/Folder bất kì trong thư mục gốc
* Nagios sẽ phát cảnh báo



* Trở lại trạng thái **OK** sử dụng tổ hợp Ctrl-Z trên thư mục gốc để back lại trạng thái trước đó