Học Viện Công Nghệ Bưu Chính Viễn Thông

Sinh viên: Nguyễn Quốc Đạt

Lớp: An toàn thông tin D14CQAT01-N

MSV: N14DCAT124

BÁO CÁO CHUYÊN ĐỀ AN TOÀN MẠNG

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

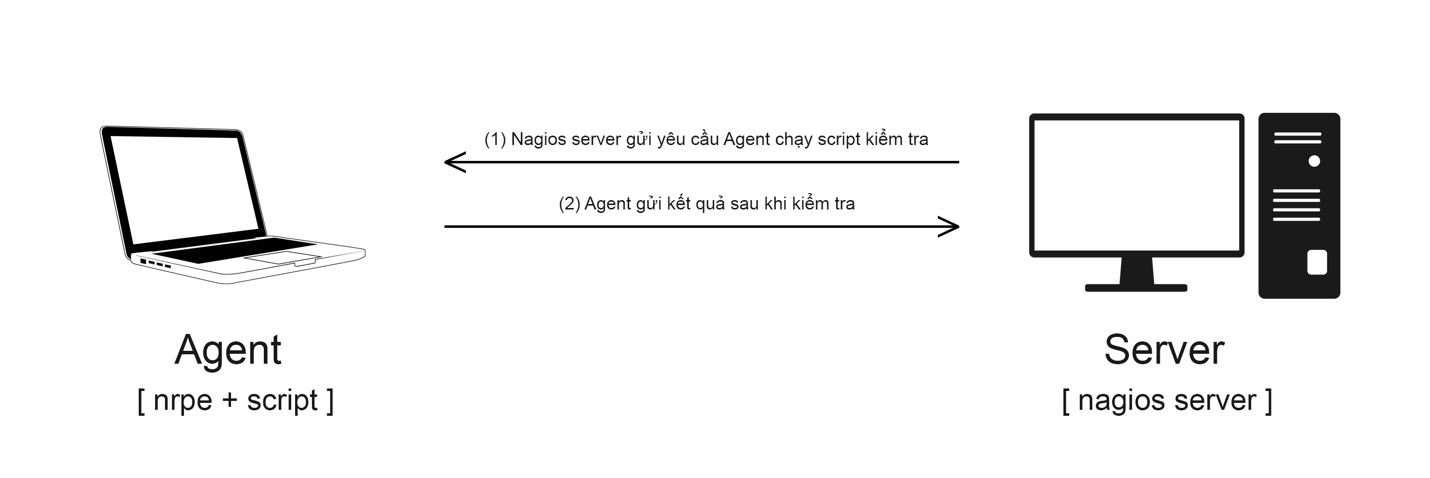
Lời mở đầu

Với mức độ xâm nhập ngày càng cao của tin tặc, nguy cơ nội dung files, thư mục bị cài đặt những files có nội dung bất thường ngày càng cao. Do đó, vấn đề đặt ra là làm sao để phòng ngừa việc máy tính bị cài đặt những file có chứa mã độc cũng như là cách để có thể xử lý khi gặp phải những tình huống trên

Đề tài phát triển từ nhu cầu thiết thực trong việc giám sát, an ninh dữ liệu trên hệ thống máy con. Nhờ vào việc theo dõi và báo cáo những thay đổi bất thường từ phía client giúp cho quản trị viên nhận biết và phát hiện những nguy cơ bảo mật kịp thời

# 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.
* Version: Nagios-Server 4.1.1.

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:

+ OS Ubuntu 16.04.

+ Service nrpe-2.15.

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.

# II. Cài đặt

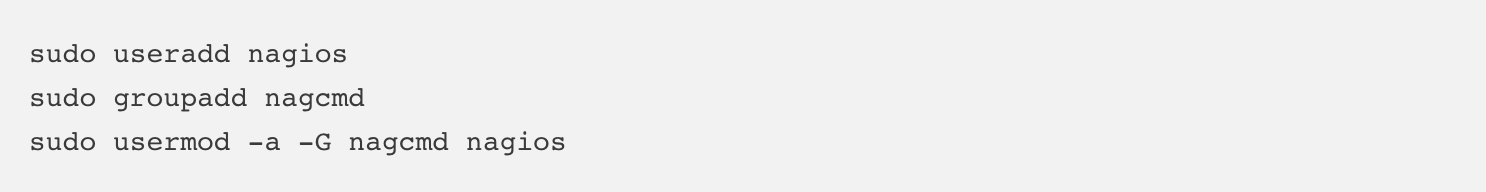
## 1. Cài đặt Nagios server cho máy chủ giám sát.

Sử dụng phiên bản Nagios server 4 để cài đặt trên máy chủ giám sát. Chú ý rằng phải đảm bảo máy chủ giám sát (server) và máy trạm được giám sát (agent) cùng miền mạng với nhau.

Quá trình cài đặt Nagios 4 được thực hiện theo trình tự các bước sau:

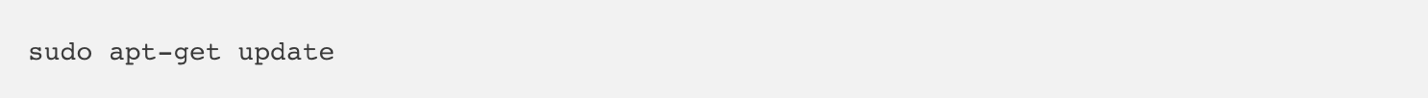
### Bước 1: Tạo user và group đảm bảo quyền thực thi cho nagios.

Tạo một user có tên là “nagios” và một group có tên là “nagcmd”. Sau đó add user nagios và group nagcmd.

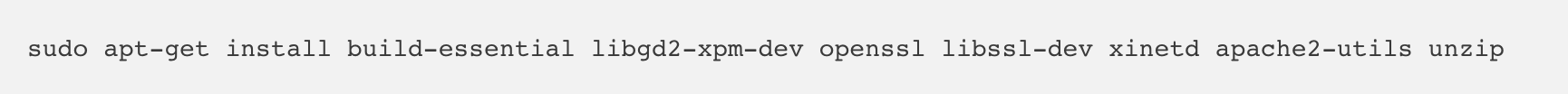


### Bước 2: Cài đặt môi trường

Cập nhật danh sách các gói cài đặt cho apt-get

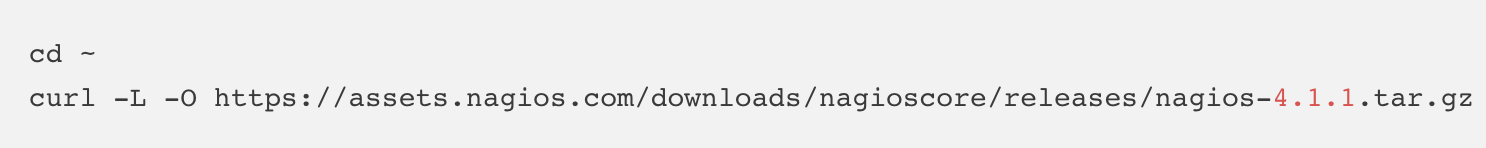


Cài đặt các gói cần thiết

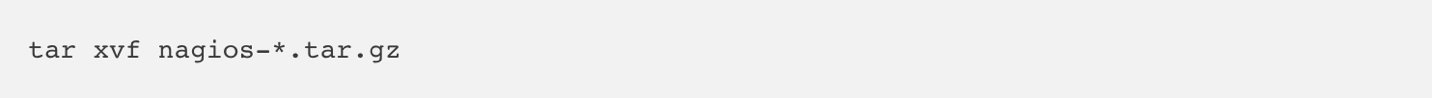


### Bước 3: Cài đặt Nagios Core

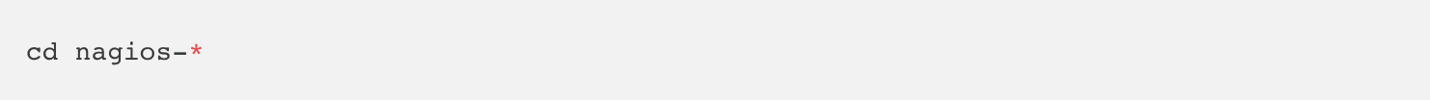
Tải gói cài đặt Nagios 4.1.1 bằng curl.



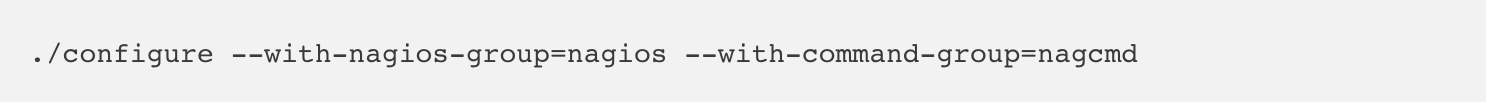
Giải nén gói cài đặt.



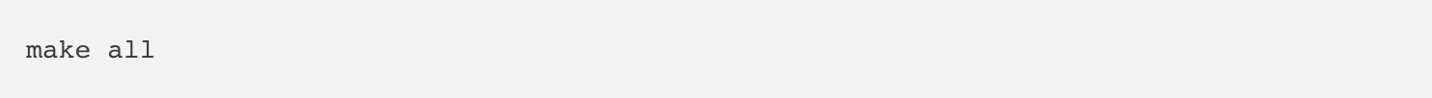
Di chuyển tới thư mục vừa được giải nén.



Thay đổi cấu hình cài đặt.



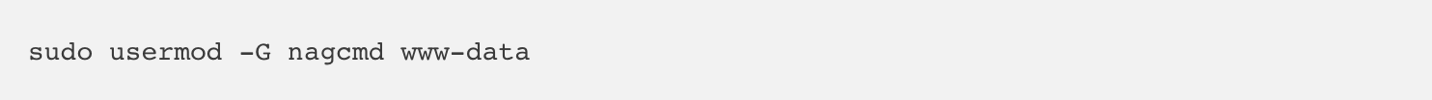
Biên dịch Nagios.



Tiến hành cài đặt Nagios.



Thêm web server www-data vào nhóm nagcmd.

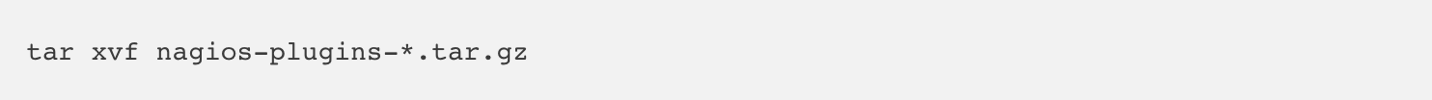


### Bước 4: Cài đặt Nagios Plugins

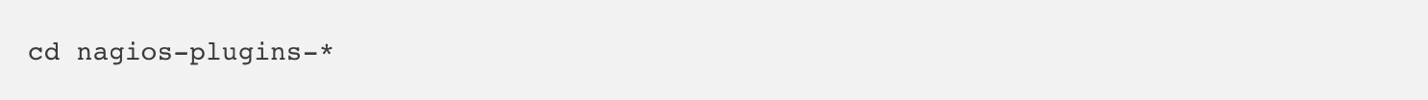
Tải gói cài đặt nagios plugins 3.1.2



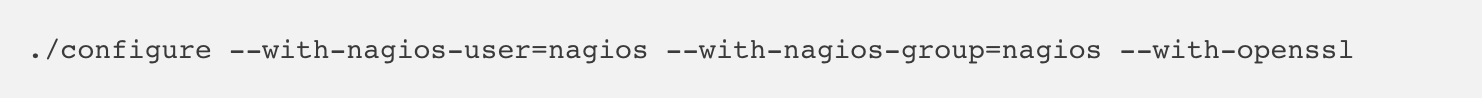
Giải nén gói cài đặt.



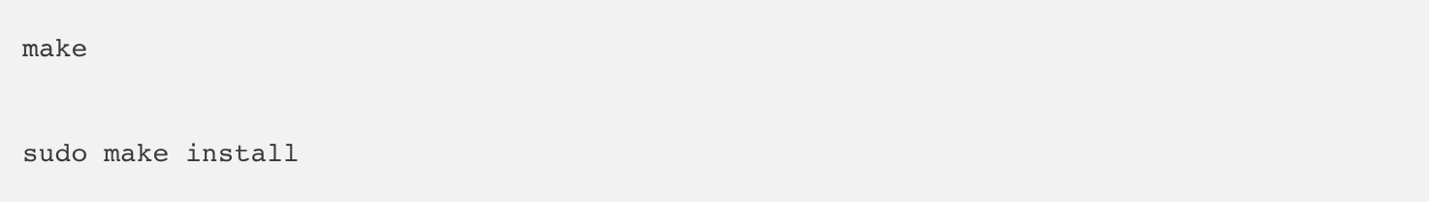
Di chuyển tới thư mục vừa được giải nén.



Cấu hình cài đặt.



Biên dịch plugins và cài đặt.



## 2. Cài đặt nrpe cho máy trạm được giám sát

Tải gói cài đặt nrpe-2.15

cd ~

curl -L -O http://downloads.sourceforge.net/project/nagios/nrpe-2.x/nrpe-2.15/nrpe-2.15.tar.gz

Giải nén mã nguồn

tar xvf nrpe-\*.tar.gz

Định nghĩa cấu hình NRPE

./configure --enable-command-args --with-nagios-user=nagios --with-nagios-group=nagios --with-ssl=/usr/bin/openssl --with-ssl-lib=/usr/lib/x86\_64-linux-gnu

Cài đặt NRPE

make all

sudo make install

sudo make install-xinetd

sudo make install-daemon-config

Thay đổi file cấu hình: Tìm dòng only\_from và thêm IP của Nagios Server vào file:

/etc/xinetd.d/nrpe

Khởi động lại dịch vụ xinetd

sudo service xinetd restart

### Tổ chức cấu hình Nagios

Tìm và bỏ ký tự commant # trong file cấu hình /usr/local/nagios/etc/nagios.cfg có dòng như sau:

#cfg\_dir=/usr/local/nagios/etc/servers

Bây giờ tạo thư mục lưu trữ tệp cấu hình cho mỗi máy mà server sẽ giám sát

sudo mkdir /usr/local/nagios/etc/servers

### Định cấu hình lệnh check\_nrpe

Thêm lệnh mới vào file cấu hình Nagios: /usr/local/nagios/etc/objects/commands.cfg. Thêm phần sau vào cuối tệp:

define command{

command\_name check\_folder

command\_line $USER1$/check\_nrpe -H $HOSTADDRESS$ -c check\_folder

}

### Định dạng Apache

Bật mô-đun viết lại và cgi của Apache:

sudo a2enmod rewrite

sudo a2enmod cgi

Tạo admin user với uesrname = “nagiosadmin”

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

Bây giờ tạo một liên kết tượng trưng của nagios.conf đến thư mục sites-enabled:

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

Khởi động lại nagios và apcahe

sudo service nagios start

sudo service apache2 restart

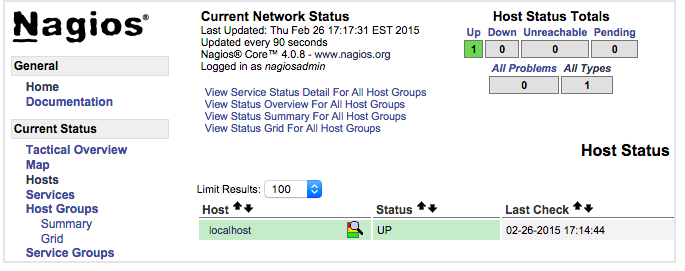
kích hoạt Nagios để khởi động máy chủ

sudo ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios

Truy cập vào giao diện web Nagios

Truy cập bằng trình duyệt với địa chỉ: http://nagios\_server\_public\_ip/nagios

Đăng nhập vằng tài khoản “nagiosadmin” đã tạo trước đó

Như vậy là đã cấu hình Nagios Server thành công, kế tiếp sẽ add agent vào để Server có thể giám sát máy Agent

## 3. Xây dựng chương trình giám sát

Trên máy Agent cài đặt Nagios Plugins và NRPE:

sudo apt-get update

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

### Định cấu hình Allowed Hosts

Tìm chỉ thị allowed\_hosts và thêm địa chỉ IP riêng của máy chủ Nagios vào danh sách ở file /etc/nagios/nrpe.cfg

### Định dạng lệnh Allowed NRPE

Truy cập file /etc/nagios/nrpe.cfg

Thay đổi nội dung của ba dòng sau:

server\_address=client\_private\_IP

allowed\_hosts=nagios\_server\_private\_IP

command[check\_folder2]=sudo /usr/lib/nagios/plugins/monitor\_folder.pl

Khởi động lại NRPE

sudo service nagios-nrpe-server restart

### Thêm máy chủ lưu trữ vào cấu hình Nagios

Trên máy chủ Nagios, tạo một tệp cấu hình mới cho mỗi máy agent

sudo vi /usr/local/nagios/etc/servers/yourhost.cfg

với yourhost = “tên máy client”

với nội dung:

define host {

use linux-server

host\_name datshiro2

alias Ubuntu Agent

address 10.0.2.6

}

define service{

use local-service

host\_name datshiro2

service\_description Check folder

check\_command check\_folder

check\_interval 1

}

Sau đó nạp lại Nagios

sudo service nagios reload

## 4. Tích hợp chương trình giám sát vào Nagios

Ở máy Agent, add file script thực thi lệnh kiểm tra cây thư mục của folder vào đường dẫn **/usr/lib/nagios/plugins/** và đặt tên “check\_folder.pl”

Add quyền thực thi vào file

Sudo chmod +x /usr/lib/nagios/plugins/check\_folder.pl

### Code Script - check\_folder.pl

#!/usr/bin/perl

use strict;

use warnings;

use Digest::file qw(digest\_file\_hex);

use Digest::MD5 qw(md5 md5\_hex md5\_base64);

use File::Find;

use File::Spec::Functions;

use File::stat;

use File::Basename;

my $folder\_path;

my %map\_digest;

my $DB\_FOLDER\_PATH = File::Spec->rel2abs("home/datshiro-2/db");

my $first\_time = 0;

if(!-e $DB\_FOLDER\_PATH){

mkdir $DB\_FOLDER\_PATH;

$first\_time = 1;

}

$folder\_path = "home/datshiro-2/Downloads" ;

$folder\_path = File::Spec->rel2abs($folder\_path);

print "folder\_path: $folder\_path\n";

######## Check Hash Changed

my $check\_delete = checkDeletedFiles($folder\_path, 0);

my $check\_changed = checkHashChanged($folder\_path, 0);

hashFiles($folder\_path);

#my $check\_delete = 0;

#my $check\_changed = 1;

print "Result:";

if($first\_time == 1){

print "Run first time!\n";

exit (0);

}

if ($check\_delete != 0 || $check\_changed != 0){

print "Folder has changed\n";

exit(1);

}

print "No Changes!\n";

exit(0);

############################### END OF IMPLEMENT #############################

sub checkHashChanged {

my ($path, $isSubDir) = @\_;

my $changedFlag = 0;

my %map\_digest = readHashDBFile($path);

my @files = glob( $path . '/\*' );

foreach(@files){

my $file = $\_;

#$changedFlag = 0;

if((-d $file) && ($file ne $path)){

next if (basename($file) eq "db");

my $folder\_changed\_flag = checkHashChanged($file, 1);

if($folder\_changed\_flag > 0 ){

$changedFlag +=7;

}

}

#next if(-d $file);

my $file\_inode = getInode($file);

my ($name, $hash);

if(!$map\_digest{$file\_inode}){

$changedFlag = 1;

}elsif(!-d $file){

($name, $hash) = split /:/, $map\_digest{$file\_inode}, 2;

if($file ne $name){

$changedFlag += 2;

}

if(hashFile($file) ne $hash){

$changedFlag += 4;

}

}

if($changedFlag != 0 && $isSubDir == 1){

return 1;

}

}

return $changedFlag;

}

sub checkDeletedFiles{

my ($path, $isSubDir) = @\_;

my $changedFlag = 0;

my %map\_digest = readHashDBFile($path);

foreach my $key (keys %map\_digest){

my $path\_inode = findPathByInode($path, $key);

#$changedFlag = 0;

#print "file '$path\_inode' \n";

if((-d $path\_inode) && ($path\_inode ne $path)){

next if (basename($path\_inode) eq "db");

my $folder\_changed\_flag = checkDeletedFiles($path\_inode, 1);

if($folder\_changed\_flag > 0){

#print "Folder $path\_inode has deleted files\n";

$changedFlag += 1;

}

}

if(!-e $path\_inode){

$changedFlag += 1;

}

}

return $changedFlag;

}

sub getAbs{

my ($path) = @\_;

return File::Spec->rel2abs($path);

}

sub getInode{

my ($path) = @\_;

my $st = stat($path) or die "No $path $!";

$path = File::Spec->rel2abs($path);

return $st->ino;

}

sub findPathByInode{

my ($directory, $inode) = @\_;

my $path = `find $directory -inum $inode`;

chomp $path;

if($path){

return $path;

}

}

sub readHashDBFile{

my ($file) = @\_;

my $folder\_inode = getInode($file);

my $db\_file = catfile($DB\_FOLDER\_PATH, $folder\_inode.".chksum");

my $fh;

unless(-e $db\_file){

#Create the file if it doesn't exist

open my $fc, ">", $db\_file;

close $fc;

}

open($fh, '<', $db\_file) or die "Could not open file '$db\_file' $!";

my %map\_digest;

while(my $line = <$fh>){

chomp($line);

my ($key,$digest) = split(':', $line, 2);

$map\_digest{$key} = $digest;

}

close($fh);

return %map\_digest;

}

sub hashFiles{

my($path) = @\_;

my $path\_inode = getInode($path);

my %hash\_map;

my $db\_file = catfile($DB\_FOLDER\_PATH, basename($path\_inode).".chksum");

my $fh;

open($fh, '<', $db\_file) or die "Could not open file '$db\_file' $!";

if(<$fh>){

return;

}

close($fh);

my @files = glob( $path . '/\*' );

foreach(@files){

my $file = $\_;

if((-d $file) && ($file ne $path)){

hashFiles($file);

}

#next if(-d $file);

my $digest = "";

if(!-d $file) {

$digest = hashFile($file);

}

my $key = getInode($file);

my $value = $file.":".$digest;

$hash\_map{$key} = $value;

}

unless(-e $db\_file){

#Create the file if it doesn't exist

open my $fc, ">", $db\_file;

close $fc;

}

open(my $f, '>', $db\_file) or die "Couldn't open: $!";;

foreach my $key (keys %hash\_map){

print $f "$key:$hash\_map{$key}\n" ;

}

close($f);

}

sub hashFile{

my($path) = @\_;

if(-d $path){

return;

}

$path = getAbs($path);

my $digest = digest\_file\_hex($path, "MD5");

return $digest;

}

# III. Kết quả

### Khi chưa có sự thay đổi trong folderScreen Shot 2018-11-03 at 5.04.51 PM.pngScreen Shot 2018-11-03 at 5.05.33 PM.png

### Sau khi thao tác thay đổi cây thư mục của folderScreen Shot 2018-11-03 at 5.07.57 PM.png