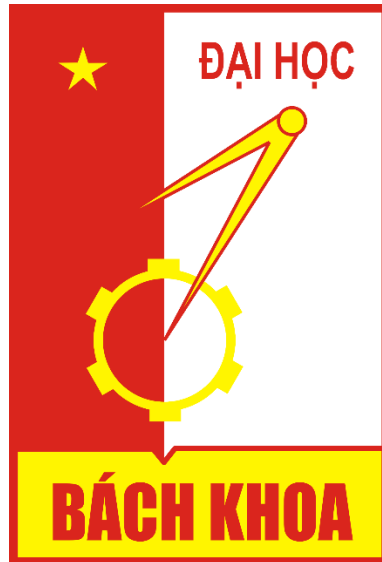


TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
Viện Công nghệ Thông tin và Truyền thông



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 bởi nếu như có một sự cố xảy ra mà người quản trị không biết hoặc hệ thống không tự khắc phục thì sẽ ảnh hưởng 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 phí 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
1.1. Giới thiệu về Nagios.....	4
1.2. Cơ chế và kiến trúc hoạt động của Nagios.	4
1.3. Hệ thống các tệp tin cấu hình.	6
1.4. Triển khai và cấu hình Nagios trên Linux.....	7
Chương 2. Thực nghiệm giám sát mạng với Nagios.....	8
2.1. Các dịch vụ giám sát	8
2.2. Đánh giá hệ thống và kết quả đạt được	10

Chương 1. Phần mềm mã nguồn mở Nagios.

1.1. 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 ...

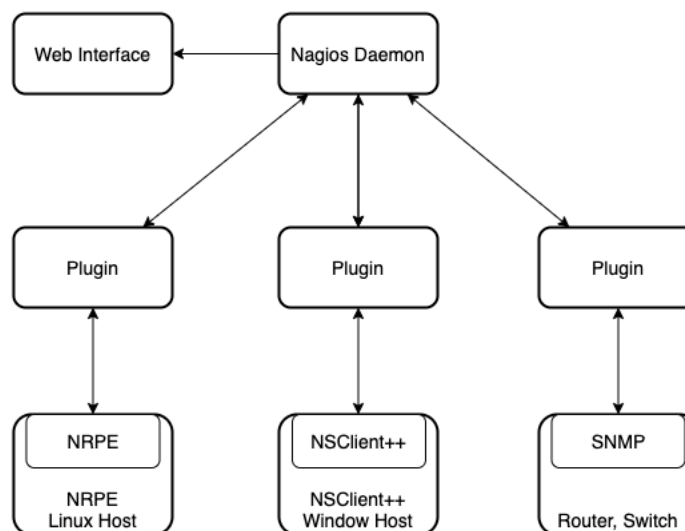
1.2. Cơ chế và kiến trúc hoạt động của Nagios.

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 cụ 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.



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 lý 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.

1.3. Hệ thống các tệp tin cấu hình.

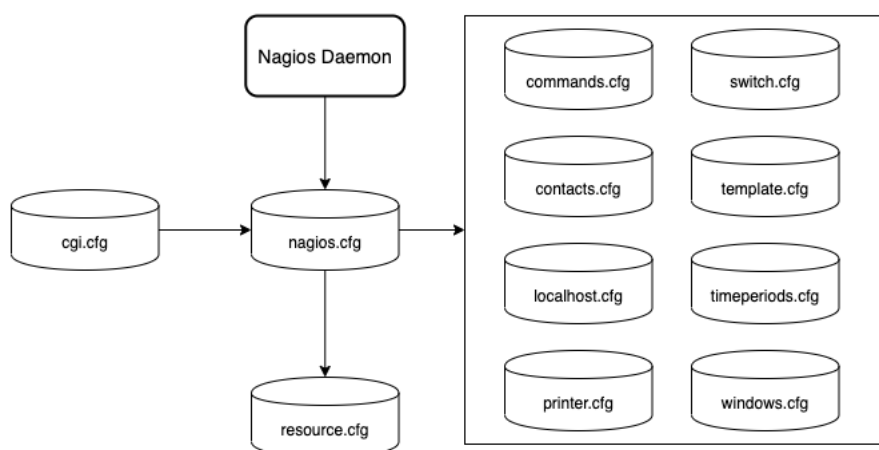
Hệ thống tệp tin của Nagios rất đơn giản, các cấu hình được lưu dưới dạng tệp tin *.cfg, tập trung chủ yếu trong thư mục `/usr/local/nagios/etc/` với các thành phần chính sau:

`nagios.cfg`: tệp tin này chứa các thông tin trỏ tới các tệp tin cấu hình khác, hoặc một thư mục chứa các tệp 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 những 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 tệp tin cấu hình chính `nagios.cfg`, tùy chỉnh các cách thức bảo mật cũng như truy cập vào hệ thống.

Ngoài 3 tệp tin chính ở trên, Nagios còn có một số tệp 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 tùy chỉnh các cấu hình phù hợp với hệ thống được giám sát.



Hình 2: Hệ thống các tệp tin cấu hình.

1.4. 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.

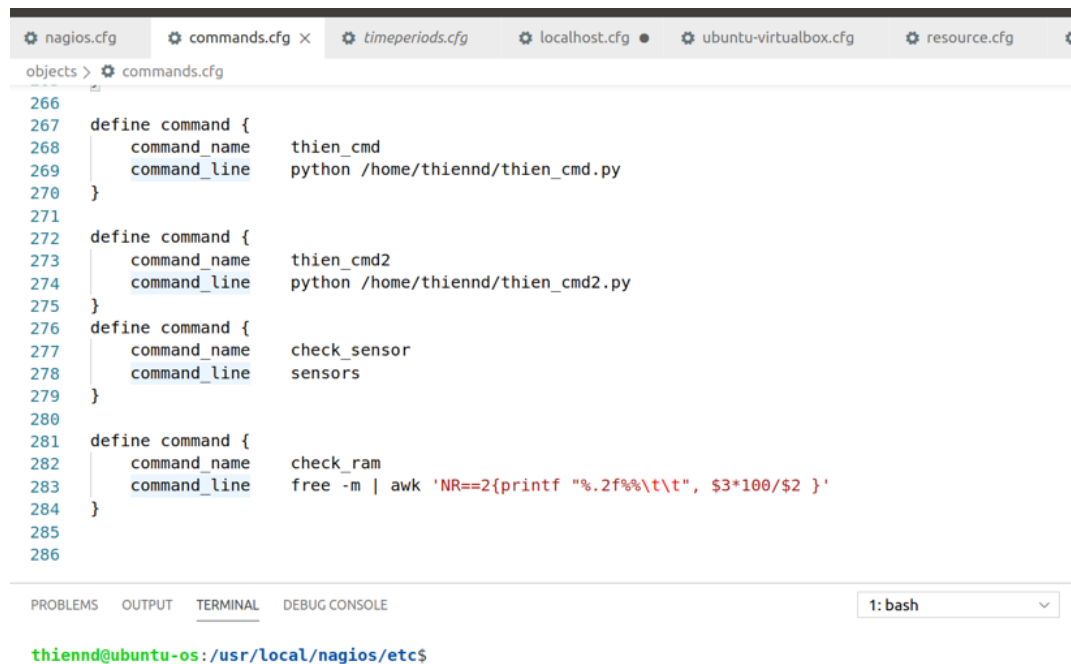
```
$ sudo make install-webconf
$ sudo a2enmod rewrite
$ sudo a2enmod cgi
$ sudo ufw allow Apache
$ sudo ufw reload
$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users
nagiosadmin
$ sudo systemctl restart apache2.service
```

- 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

Chương 2. Thực nghiệm giám sát mạng với Nagios.

2.1. Các dịch vụ giám sát

Để tùy 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 tùy biến 2 lệnh `thien_cmd`, `thien_cmd2` dùng để thực thi hai file python để in ra thông số hệ thống.



```
objects > commands.cfg
266
267 define command {
268     command_name    thien_cmd
269     command_line     python /home/thiennd/thien_cmd.py
270 }
271
272 define command {
273     command_name    thien_cmd2
274     command_line     python /home/thiennd/thien_cmd2.py
275 }
276
277 define command {
278     command_name    check_sensor
279     command_line     sensors
280 }
281
282 define command {
283     command_name    check_ram
284     command_line     free -m | awk 'NR==2{printf "%.2f%\t\t", $3*100/$2 }'
285 }
286
```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

1: bash

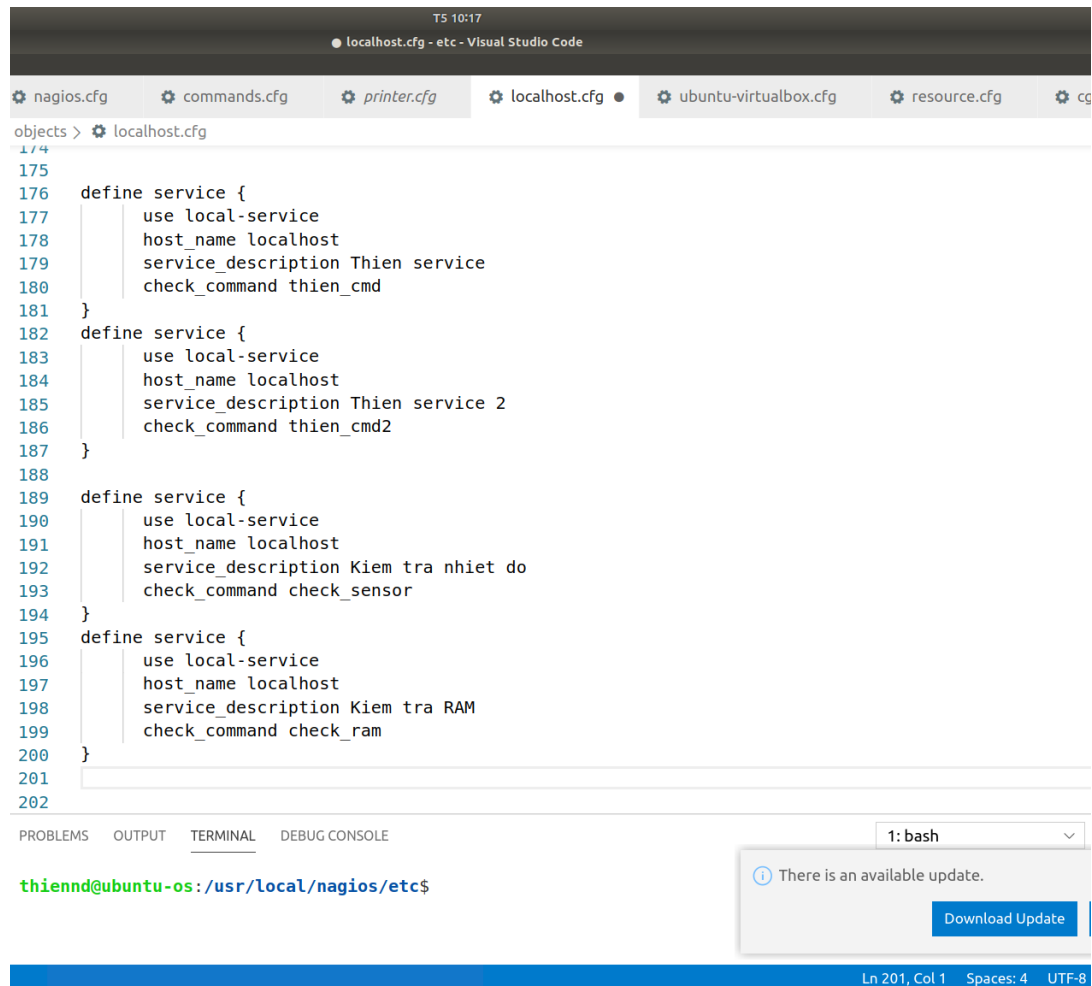
thiennd@ubuntu-os: /usr/local/nagios/etc\$

File python `thien_cmd` dùng để in ra thông số cấu hình hiện tại của hệ thống



```
home > thiennd > thien_cmd.py
1 import platform
2 machine = platform.machine()
3 version = platform.version()
4 plf = platform.platform()
5 uname = platform.uname()
6 system = platform.system()
7 processor = platform.processor()
8
9 print("Kien truc: ",machine)
10 print("Phien ban:", version)
11 print("Nen tang: ",plf)
12 print("Uname: ",uname)
13 print("He thong: ",system)
14 print("Bo xu li: ",processor)
15
```


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.



```
TS 10:17
localhost.cfg - etc - Visual Studio Code

nagios.cfg  commands.cfg  printer.cfg  localhost.cfg  ubuntu-virtualbox.cfg  resource.cfg  cg

objects > localhost.cfg
174
175
176 define service {
177     use local-service
178     host_name localhost
179     service_description Thien service
180     check_command thien_cmd
181 }
182 define service {
183     use local-service
184     host_name localhost
185     service_description Thien service 2
186     check_command thien_cmd2
187 }
188
189 define service {
190     use local-service
191     host_name localhost
192     service_description Kiem tra nhiet do
193     check_command check_sensor
194 }
195 define service {
196     use local-service
197     host_name localhost
198     service_description Kiem tra RAM
199     check_command check_ram
200 }
201
202
```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

thiennd@ubuntu-os:/usr/local/nagios/etc\$

1: bash

There is an available update.

Download Update

Ln 201, Col 1 Spaces: 4 UTF-8

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 hiện thị ở trạng thái active (running), còn không thì sẽ báo lỗi thiết lập.

```

thiennd@ubuntu-os: ~
File Edit View Search Terminal Help
nagios.service - Nagios Core 4.4.5
Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: e
Active: active (running) since Thu 2020-06-18 10:20:21 +07; 25s ago
Docs: https://www.nagios.org/documentation
Process: 9357 ExecStopPost=/bin/rm -f /usr/local/nagios/var/rw/nagios.cmd (cod
Process: 9356 ExecStop=/bin/kill -s TERM ${MAINPID} (code=exited, status=0/SUC
Process: 9359 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/
Process: 9358 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/e
Main PID: 9360 (nagios)
Tasks: 10 (limit: 4915)
CGroup: /system.slice/nagios.service
└─9360 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.c
─9361 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw
─9362 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw
─9363 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw
─9364 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw
─9365 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw
─9366 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw
─9367 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.c
─9368 /usr/local/nagios/libexec/check_ping -H 192.168.56.104 -w 3000
─9369 /bin/ping -n -U -W 30 -c 5 192.168.56.104

Thg 6 18 10:20:21 ubuntu-os nagios[9360]: qh: help for the query handler regist
Thg 6 18 10:20:21 ubuntu-os nagios[9360]: wproc: Successfully registered manager
Thg 6 18 10:20:21 ubuntu-os nagios[9360]: wproc: Registry request: name=Core Wor
Thg 6 18 10:20:21 ubuntu-os nagios[9360]: wproc: Registry request: name=Core Wor
Thg 6 18 10:20:21 ubuntu-os nagios[9360]: wproc: Registry request: name=Core Wor
Thg 6 18 10:20:21 ubuntu-os nagios[9360]: wproc: Registry request: name=Core Wor
Thg 6 18 10:20:21 ubuntu-os nagios[9360]: wproc: Registry request: name=Core Wor
Thg 6 18 10:20:21 ubuntu-os nagios[9360]: wproc: Registry request: name=Core Wor
Thg 6 18 10:20:21 ubuntu-os nagios[9360]: SERVICE FLAPPING ALERT: home-router;PI
lines 1-31

```

2.2.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

Nagios®

Current Network Status
 Last Updated: Thu Jun 18 10:28:37 +07 2020
 Updated every 90 seconds
 Nagios® Core™ 4.4.5 - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
12	1	1	0	0

Service Status Details For Host 'localhost'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Bang thong mạng	UNKNOWN	06-18-2020 10:26:59	11d 22h 31m 40s	4/4	(No output on stdout) stderr:
	Current Load	OK	06-18-2020 10:26:59	17d 16h 6m 12s	1/4	OK - load average: 0.26, 0.43, 0.32
	Current Users	OK	06-18-2020 10:26:59	56d 11h 48m 32s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	06-18-2020 10:26:59	56d 11h 47m 55s	1/4	HTTP OK: HTTP/1.1 200 OK - 11192 bytes in 0.000 second response time
	Kiem tra RAM	OK	06-18-2020 10:26:59	15d 5h 30m 5s	1/4	16.65%
	Kiem tra nhiet do	OK	06-18-2020 10:26:59	15d 5h 39m 42s	1/4	thinkpad-isa-0000
	PING	OK	06-18-2020 10:26:59	15d 7h 48m 47s	1/4	PING OK - Packet loss = 0%, RTA = 0.19 ms
	Root Partition	OK	06-18-2020 10:26:59	56d 11h 46m 40s	1/4	DISK OK - free space: / 14684 MB (24.67% inode=93%);
	SSH	OK	06-18-2020 10:26:59	17d 15h 44m 39s	1/4	SSH OK - OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 (protocol 2.0)
	Swap Usage	OK	06-18-2020 10:26:59	56d 11h 45m 25s	1/4	SWAP OK - 100% free (2047 MB out of 2047 MB)
	Thien service	OK	06-18-2020 10:26:59	15d 5h 56m 55s	1/4	(Kien truc: ', x86_64')
	Thien service 2	WARNING	06-18-2020 10:26:59	15d 5h 36m 15s	4/4	(No output on stdout) stderr: Traceback (most recent call last):
	Total Processes	OK	06-18-2020 10:26:59	17d 15h 46m 0s	1/4	PROCS OK: 91 processes with STATE = RSZDT
	Uptime	OK	06-18-2020 10:26:59	15d 5h 33m 0s	1/4	Uptime OK: 0 day(s) 0 hour(s) 53 minute(s)

Page Tour

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, UNKNOWN, 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.

The screenshot shows the Nagios web interface in a Mozilla Firefox browser. The page displays the status of a service named 'Kiem tra nhiet do' (Temperature Check) on the host 'localhost'. The service is currently in an 'OK' state, having been last updated on June 18, 2020, at 10:31:58. The interface includes a sidebar with navigation links for General, Current Status, and Reports. The main content area shows service information, service state information (including a list of temperatures for various sensors), and service commands. A 'Page Tour' button is visible on the right side of the interface.

Service Information

Last Updated: Thu Jun 18 10:31:58 +07 2020
Updated every 90 seconds
Nagios® Core™ 4.4.5 - www.nagios.org
Logged in as nagiosadmin

Service
Kiem tra nhiet do
On Host
localhost
(localhost)

Member of
No servicegroups.

127.0.0.1

Service State Information

Current Status: OK (for 15d 5h 43m 3s)
Status Information:
thinkpad-isa-0000
Adapter: ISA adapter
fan1: 0 RPM
temp1: +49.0°C
temp2: N/A
temp3: +0.0°C
temp4: +0.0°C
temp5: +0.0°C
temp6: +0.0°C
temp7: +0.0°C
temp8: +0.0°C
temp9: +0.0°C
temp10: +1.0°C
temp11: +0.0°C
temp12: +0.0°C
temp13: +0.0°C
temp14: +0.0°C
temp15: +0.0°C
temp16: +0.0°C

Service Commands

- ✗ Disable active checks of this service
- 🕒 Re-schedule the next check of this service
- ❓ Submit passive check result for this service
- ✗ Stop accepting passive checks for this service
- ✗ Stop obsessing over this service
- ✗ Disable notifications for this service
- 📧 Send custom service notification
- 🕒 Schedule downtime for this service
- ✗ Disable event handler for this service
- ✗ Disable flap detection for this service
- ✗ Clear flapping state for this service

Với một dịch vụ bị lỗi thì ta cần kiểm tra lại các lệnh commands và thông số cấu hình của dịch vụ, tùy 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.

Service State Information

Current Status: **WARNING** (for 15d 5h 42m 52s)
Status Information: (No output on stdout) stderr: Traceback (most recent call last):
File "/home/thiennd/thien_cmd2.py", line 9, in <module>
total, used, free = shutil.disk_usage("/")
AttributeError: 'module' object has no attribute 'disk_usage'
Performance Data:
Current Attempt: 4/4 (HARD state)
Last Check Time: 06-18-2020 10:31:59
Check Type: ACTIVE
Check Latency / Duration: 0.000 / 0.023 seconds
Next Scheduled Check: 06-18-2020 10:36:59
Last State Change: 06-03-2020 04:52:22
Last Notification: 06-18-2020 10:31:59 (notification 11)
Is This Service Flapping? **NO** (0.00% state change)
In Scheduled Downtime? **NO**
Last Update: 06-18-2020 10:35:10 (0d 0h 0m 4s ago)

Active Checks: **ENABLED**
Passive Checks: **ENABLED**
Obsessing: **ENABLED**
Notifications: **ENABLED**
Event Handler: **ENABLED**
Flap Detection: **ENABLED**

Service State Information

Current Status: **OK** (for 15d 6h 3m 31s)
Status Information: ('Kien truc: ', 'x86_64')
('Phien ban:', '#53~18.04.1-Ubuntu SMP Thu Jun 4 14:58:26 UTC 2020')
('Nen tang: ', 'Linux-5.3.0-59-generic-x86_64-with-Ubuntu-18.04-bionic')
('Uname: ', ('Linux', 'ubuntu-os', '5.3.0-59-generic', '#53~18.04.1-Ubuntu SMP Thu Jun 4 14:58:26 UTC 2020', 'x86_64', 'x86_64'))
('He thong: ', 'Linux')
('Bo xu li: ', 'x86_64')
Performance Data:
Current Attempt: 1/4 (HARD state)
Last Check Time: 06-18-2020 10:31:59
Check Type: ACTIVE
Check Latency / Duration: 0.000 / 0.023 seconds
Next Scheduled Check: 06-18-2020 10:36:59
Last State Change: 06-03-2020 04:31:42
Last Notification: N/A (notification 0)
Is This Service Flapping? **NO** (0.00% state change)
In Scheduled Downtime? **NO**
Last Update: 06-18-2020 10:35:10 (0d 0h 0m 3s ago)

Active Checks: **ENABLED**
Passive Checks: **ENABLED**
Obsessing: **ENABLED**
Notifications: **ENABLED**