|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **BỘ THÔNG TIN VÀ TRUYỀN THÔNG**  **HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  ------------------------------    **ĐỀ CƯƠNG**  **THỰC TẬP CƠ SỞ**  ***Đề tài*:**  **TRIỂN KHAI HỆ THỐNG**  **GIÁM SÁT MẠNG VỚI NAGIOS**  **Giảng viên hướng dẫn : TS. HUỲNH TRỌNG THƯA**  **ThS. HUỲNH THANH TÂM**  **Nhóm SV thực hiện : NHÓM 7**   |  |  | | --- | --- | | **TRẦN ANH DŨNG** | **N19DCAT013** | | **NGUYỄN QUANG CHÍNH** | **N19DCAT011** | | **MAI THẾ CHUYỂN EM** | **N19DCAT018** | | **NGUYỄN HOÀNG ĐẠI NGHĨA** | **N19DCAT054** | | **ĐẶNG ANH QUÂN** | **N19DCAT064** | | **TRẦN THANH TRA** | **N19DCAT089** |   **Lớp :**  **D19CQAT01-N**  **Khoá** **: 2019 – 2024**  **Hệ** **: ĐẠI HỌC CHÍNH QUY**  **TP.HCM, 03/2022** |

**MỤC LỤC**

[**LỜI CẢM ƠN 3**](#_heading=h.4i7ojhp)

[**LỜI MỞ ĐẦU 4**](#_heading=h.2xcytpi)

[**CHƯƠNG 1: CƠ SỞ LÝ THUYẾT 5**](#_heading=h.1ci93xb)

[***1.1***](#_heading=h.3whwml4) ***Giám sát mạng 5***

[1.1.1 Các yếu tố cơ bản trong giám sát mạng 5](#_heading=h.qsh70q)

[1.1.2 Chức năng của giám sát mạng 6](#_heading=h.3as4poj)

[1.1.3 Cần giám sát những gì 6](#_heading=h.1pxezwc)

[1.1.4 Tầm quan trọng của giám sát mạng 7](#_heading=h.49x2ik5)

[***1.2***](#_heading=h.2p2csry) ***Nagios 7***

[1.2.1 Khái niệm về Nagios 7](#_heading=h.147n2zr)

[1.2.2 Chức năng của Nagios 9](#_heading=h.ihv636)

[1.2.3 Đặc điểm Nagios 10](#_heading=h.32hioqz)

[1.2.4 Kiến trúc và tổ chức hoạt động 10](#_heading=h.1hmsyys)

[***1.3***](#_heading=h.2grqrue) ***Giao thức giám sát SNMP 11***

[1.3.1 Ưu điểm 12](#_heading=h.vx1227)

[1.3.2 Nhược điểm 12](#_heading=h.3fwokq0)

[1.3.3 Điều hành SNMP 12](#_heading=h.1v1yuxt)

[1.3.4 Các phương thức của SNMP 14](#_heading=h.19c6y18)

[**CHƯƠNG 2: THIẾT KẾ HỆ THỐNG GIÁM SÁT MẠNG BẰNG PHẦN MỀM NAGIOS 15**](#_heading=h.28h4qwu)

[***2.1***](#_heading=h.nmf14n) ***Mô hình triển khai 15***

[***2.2 Giới thiệu và giải thích mô hình 16***](#_heading=h.1mrcu09)

[***2.3 Cấu hình Nagios 16***](#_heading=h.46r0co2)

[2.3.1 Các tệp cấu hình chương trình 16](#_heading=h.2lwamvv)

[2.3.2 Các tệp cấu hình đối tượng 16](#_heading=h.111kx3o)

[2.3.3 Định nghĩa host 17](#_heading=h.206ipza)

[2.3.4 Định nghĩa dịch vụ 17](#_heading=h.2zbgiuw)

[2.3.5 Định nghĩa lệnh 18](#_heading=h.3ygebqi)

[2.3.6 Cấu hình Nagios Server 19](#_heading=h.2dlolyb)

[**CHƯƠNG 3: ỨNG DỤNG THỰC NGHIỆM 21**](#_heading=h.4bvk7pj)

[***3.1***](#_heading=h.2r0uhxc) ***Kịch bản 1: Sự cố Mail Server 21***

[***3.2***](#_heading=h.3q5sasy) ***Kịch bản 2: Sự cố Web Server 22***

[***3.3***](#_heading=h.1jlao46) ***Kịch bản 3: Sự cố với Client 23***

[***3.4 Nhận định kết quả 25***](#_heading=h.3hv69ve)

[**KẾT LUẬN 25**](#_heading=h.1x0gk37)

[**TÀI LIỆU THAM KHẢO 26**](#_heading=h.4h042r0)

**DANH MỤC HÌNH ẢNH**

[Hình 1: Hệ thống giám sát mạng 5](#_heading=h.2bn6wsx)

[Hình 2: Nagios 8](#_heading=h.3o7alnk)

[Hình 3: Các đối tượng cần giám sát trên Nagios 9](#_heading=h.23ckvvd)

[Hình 4: Sơ đồ tổ chức của Nagios 11](#_heading=h.41mghml)

[Hình 5: Mô hình giao thức hoạt động SNMP 13](#_heading=h.4f1mdlm)

[Hình 6: Hoạt động của giao thức SNMP 13](#_heading=h.2u6wntf)

[Hình 7: Các phương thức cơ bản của SNMP 14](#_heading=h.3tbugp1)

[Hình 8: Mô hình triển khai giám sát Nagios 15](#_heading=h.37m2jsg)

[Hình 9: Các tệp đối tượng 17](#_heading=h.3l18frh)

[Hình 10: Định nghĩa host 17](#_heading=h.4k668n3)

[Hình 11: Định nghĩa dịch vụ 18](#_heading=h.1egqt2p)

[Hình 12: Kiểm tra Warnings/Errors của hệ thống Nagios 19](#_heading=h.sqyw64)

[Hình 13: Đăng nhập Nagios Server 20](#_heading=h.3cqmetx)

[Hình 14: Giao diện giám sát Nagios 20](#_heading=h.1rvwp1q)

[Hình 15: Cảnh báo Mail Server 22](#_heading=h.1664s55)

[Hình 16: Service check http 22](#_heading=h.25b2l0r)

[Hình 17: Xây dựng kịch bản sự cố Web Server 23](#_heading=h.kgcv8k)

[Hình 18: Nagios báo cáo cảnh báo sự cố Web 23](#_heading=h.34g0dwd)

[Hình 19: Giám sát máy chạy hệ điều hành Windows 24](#_heading=h.43ky6rz)

[Hình 20: Xây dựng kịch bản sự cố Client 25](#_heading=h.2iq8gzs)

[Hình 21: Nagios báo cáo cảnh báo sự cố Client 25](#_heading=h.xvir7l)

# LỜI CẢM ƠN

Đề tài “Triển khai hệ thống mạng với Nagios” là nội dung Nhóm 07 lựa chọn để nghiên cứu và làm đồ án báo cáo học phần Thực Tập Cơ Sở thuộc chương trình đại học ngành An Toàn Thông Tin tại trường Học Viện Công Nghệ Bưu Chính Viễn Thông – Cơ Sở Tại Thành Phố Hồ Chí Minh.

Để hoàn thành quá trình nghiên cứu và hoàn thiện đồ án học phần này, lời đầu tiên Nhóm 07 xin gửi lời cảm ơn chân thành tới quý Thầy, Cô, bạn bè của Học Viện Công Nghệ Bưu Chính Viễn Thông.

Bày tỏ lòng biết ơn sâu sắc nhất đến thầy, cô trong khoa Công Nghệ Thông Tin đã dìu dắt, chia sẻ những kiến thức quý báu trong suốt quá trình học tập tại trường. Đặc biệt là Thầy TS. Huỳnh Trọng Thưa, ThS. Huỳnh Thanh Tâm cùng với tri thức và tâm huyết của Thầy đã tạo điều kiện cho Nhóm 07 hoàn thành đồ án.

Cuối cùng, Nhóm 07 xin cảm ơn những người thân, bạn bè luôn động viên, sẽ chia, giúp đỡ, cổ vũ tinh thần… Đó là nguồn động lực giúp Nhóm 07 hoàn thành tốt đồ án học phần này.

Tp. Hồ Chí Minh, ngày 23 tháng 03 năm 2022

Nhóm 07

(Đại diện Trần Anh Dũng)

Trần Anh Dũng

# LỜI MỞ ĐẦU

Nền công nghệ thông tin nước ta đã và đang phát triển trên mọi lĩnh vực của cuộc sống. Với việc phát triển nhanh mạng lưới thiết bị công nghệ thông tin đã gây ra những khó khăn nhất định trong việc quản lý hệ thống mạng. Do đó vấn đề quản trị mạng hiện nay là không thể thiếu được. Tùy thuộc vào các giải pháp công nghệ và các ứng dụng triển khai mà các nhà khai thác lựa chọn và xây dựng các hệ thống quản lý mạng thích hợp để nâng cao hiệu quả vận hành và khai thác mạng.

Bên cạnh đó rất nhiều phần mềm hỗ trợ nhau quản lý và giám sát mạng ra đời. Nagios là hệ thống giám sát mạng có chi phí đầu tư thấp. Tuy nhiên nó có khả năng rất mạng mẽ trong việc giám sát hoạt động của các thiết bị trên mạng. Bởi vậy Nagios rất được tin tưởng và sử dụng rộng rãi trên toàn cầu. Đây là bộ công cụ hỗ trợ đắc lực cho nhà quản trị nhằm phân tích, giám sát cũng như các công cụ quản lý việc thực thi trên hệ thống mạng. Vì vậy, trong đề tài này **Nhóm 07** sẽ đi sâu tìm hiểu về ***“Hệ thống giám sát mạng với Nagios".***

# CHƯƠNG 1: CƠ SỞ LÝ THUYẾT

## Giám sát mạng

Giám sát hệ thống mạng là giám sát, thu nhập thông tin đưa ra các thành phần của hệ thống, phân tích các thông tin, dấu hiệu nhằm đánh giá và đưa ra các cảnh báo cho người quản trị hệ thống. Đối tượng của hệ thống giám sát gồm: các máy trạm, cơ sở dữ liệu, các ứng dụng, các server, các thiết bị mạng...

Khi phụ trách hệ thống mạng máy tính, để giảm thiểu tối đa các sự cố làm gián đoạn hoạt động của hệ thống mạng, người quản trị hệ thống mạng cần phải nắm bắt được tình hình sức khỏe của các thiết bị, dịch vụ được triển khai để có những quyết định xử lý kịp thời và hợp lý nhất. Ngoài ra, việc hiểu rõ tình trạng hoạt động của các thiết bị, các kết nối mạng… cũng giúp cho người quản trị tối ưu được hiệu năng hoạt động của hệ thống mạng để đảm bảo được các yêu cầu sử dụng của người dùng. Việc giám sát hoạt động của các thiết bị mạng, ứng dụng và dịch vụ trong môi trường mạng, với hàng chục hay hàng trăm thiết bị, mà người quản trị thực hiện thủ công sẽ không mạng lại hiệu quả. Vì thế, cần phải có một phần mềm thực hiện việc giám sát một cách tự động và cung cấp các thông tin cần thiết để người quản trị nắm được hoạt động của hệ thống mạng, đó là hệ thống giám sát mạng.



**Hình 1: Hệ thống giám sát mạng**

Hệ thống giám sát mạng (Network Monitoring System) là một phần mềm thực hiện việc giám sát hoạt động của hệ thống và các dịch vụ, ứng dụng bên trong hệ thống mạng đó. Nó thực hiện việc thu nhập thông tin của các thiết bị mạng, các kết nối, các ứng dụng và dịch vụ bên trong hệ thống mạng để phân tích và đưa ra các thông tin hỗ trợ người quản trị mạng có cái nhìn tổng quan, chi tiết về môi trường mạng. Dựa trên những thông tin thu nhập được, hệ thống giám sát mạng có thể tổng hợp thành các báo cáo, gửi các cảnh báo cho người quản trị để có hướng xử lý phù hợp nhằm giảm thiểu sự cố và nâng cao hiệu suất mạng. Với những thông tin nhận được từ hệ thống giám sát mạng, người quản trị có thể xử lý các sự cố và đưa ra các hướng nâng cấp thiết bị, dịch vụ để đảm bảo hệ thống mạng hoạt động thông suốt.

### 1.1.1 Các yếu tố cơ bản trong giám sát mạng

Để việc giám sát mạng đạt hiệu quả cao nhất, cần xác định các yếu tố cốt lõi của giám sát mạng như:

* Các đơn vị, hệ thống, thiết bị, dịch vụ cần giám sát.
* Các trang thiết bị, giải pháp, phần mềm thương mại phục vụ giám sát.
* Xác định các phần mềm nội bộ và phần mềm mã nguồn mở phục vụ giám sát.
* Ngoài ra, yếu tố con người, đặc biệt là quy trình phục vụ giám sát là vô cùng quan trọng.

### 1.1.2 Chức năng của giám sát mạng

* Cảnh báo qua Web, Email và SMS khi phát hiện tấn công vào hệ thống mạng.
* Báo động bằng âm thanh và SMS khi một host (Server, Router, Switch...) hoặc một dịch vụ mạng ngừng hoạt động.
* Giám sát lưu lượng mạng qua các cổng giao tiếp trên Router, Switch, Server... hiển thị qua các đồ thị trực quan, thời gian thực. Giám sát lưu lượng giữa các thiết bị kết nối với nhau một cách trực quan.

### 1.1.3 Cần giám sát những gì

Đối với hệ thống mạng, điều quan trọng nhất là nắm được các thông tin chính xác nhất vào mọi thời điểm. Tầm quan trọng chính là nắm bắt thông tin trạng thái của thiết bị vào thời điểm hiện tại, cũng như biết được thông tin về các dịch vụ, ứng dụng của hệ thống.

Thông tin sau đây chứa một vài nội dùng trạng thái hệ thống mà ta phải biết và lý do tại sao:

|  |  |
| --- | --- |
| **Cần giám sát gì** | **Tại sao** |
| Tính sẵn sàng của thiết bị (Router, Switch, Server...). | Đây là những thành phần chủ chốt giữ cho mạng hoạt động. |
| Các dịch vụ trong hệ thống (DNS, FTP, HTTP...). | Những dịch vụ này đóng vai trò quan trọng trong một cơ quan, tổ chức, nếu các dịch vụ này không được đảm bảo hoạt động bình thường và liên tục, nó sẽ ảnh hưởng nghiêm trọng đến cơ quan tổ chức đó. |
| Tài nguyên hệ thống. | Các ứng dụng đều đòi hỏi tài nguyên hệ thống, việc giám sát tài nguyên sẽ đảm bảo cho chúng ta có những can thiệp kịp thời, tránh ảnh hưởng đến hệ thống. |
| Lưu lượng trong mạng. | Nhằm đưa ra những giải pháp, ngăn ngừa hiện tượng quá tải trong mạng. |
| Các chức năng về  bảo mật. | Nhằm đảm bảo an ninh trong hệ thống. |
| Lượng dữ liệu vào  và ra của Router. | Cần xác định chính xác thông tin lượng dữ liệu để tránh quá tải hệ thống. |
| Các sự kiện được viết ra log như WinEvent or  Syslog. | Có thể thu được thông tin chính xác các hiện tượng trong hệ thống. |
| Nhiệt độ, thông tin về máy chủ, máy in. | Ta có thể biết được thông tin về máy in bị hư hỏng hay cần thay mực trước khi được người dùng báo cũng như đảm bảo máy chủ không bị quá nóng. |

10 lý do hàng đầu cho việc cần thiết phải sử dụng hệ thống giám sát mạng:

* Biết được những gì đang xảy ra trên hệ thống: thông báo tình trạng hoạt động cũng như tài nguyên hệ thống.
* Lên kế hoạch nâng cấp, sửa chữa
* Chẩn đoán các vấn đề một cách nhanh chóng
* Xem xét những gì đang hoạt động
* Biết được khi nào cần áp dụng các giải pháp sao lưu phục hồi
* Đảm bảo hệ thống bảo mật hoạt động tốt
* Theo dõi hoạt động của các tài nguyên dịch vụ trên hệ thống
* Được thông báo về tình trạng hệ thống ở khắp mọi nơi
* Đảm bảo hệ thống hoạt động liên tục
* Tiết kiệm tiền

### 1.1.4 Tầm quan trọng của giám sát mạng

Hệ thống giám sát mạng đóng vai trò quan trọng, không thể thiếu trong hạ tầng công nghệ thông tin của các cơ quan, đơn vị, tổ chức. Hệ thống này cho phép thu nhập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ các sự kiện an toàn mạng được sinh ra trong hệ thống công nghệ thông tin của tổ chức. Ngoài ra, hệ thống giám sát an toàn mạng phát hiện kịp thời các tấn công mạng, các điểm yếu, lỗ hổng bảo mật của các thiết bị, ứng dụng và dịch vụ trong hệ thống, phát hiện kịp thời sự bùng nổ virus trong hệ thống mạng, các máy tính bị nhiễm mã độc.

Hệ thống giám sát mạng sẽ giúp định hướng trong môi trường mạng phức tạp, đưa ra các báo cáo và các nhận định để đảm bảo công tác giám sát mạng an toàn hiệu quả. Thông qua hệ thống giám sát mạng giúp cho người quản trị hệ thống:

* Tính bảo mật
* Khả năng xử lý sự cố
* Tiết kiệm thời gian và tiền bạc
* Lập kế hoạch thay đổi

**Những lợi ích của việc xây dựng hệ thống giám sát mạng**

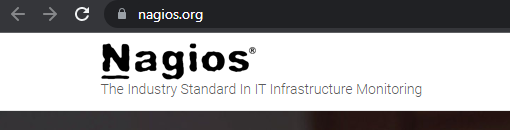
* Phát hiện sự cố, kết nối thất bại của hệ thống, dịch vụ hay thiết bị mạng 24/7 và gửi các thông tin tới người quản trị.
* Thay thế thiết bị quá tải trước khi nó ảnh hưởng đến hệ thống.
* Tìm ra bất thường trong mạng có thể dẫn đến mối đe dọa an ninh.
* Giải quyết hiệu quả về việc bị lấy cắp thông tin.

## Nagios

### 1.2.1 Khái niệm về Nagios

Nagios là một hệ thống giám sát mạnh mẽ cho phép các tổ chức xác định và giải quyết các vấn đề cơ sở hạ tầng CNTT trước khi chúng ảnh hưởng nghiêm trọng đến quá trình kinh doanh.

Ra mắt đầu tiên 1990, Nagios đã phát triển với hàng ngàn dự án được phát triển bởi cộng đồng Nagios trên toàn thế giới. Nagios chính thức bảo trợ bởi doanh nghiệp Nagios, hỗ trợ các cộng đồng trong một số cách khác nhau thông qua doanh số bán hàng thương mại của các sản phẩm dịch vụ.



**Hình 2: Nagios**

Nagios là một công cụ để giám sát hệ thống. Điều này có nghĩa là nó liên tục kiểm tra trạng thái của máy và dịch vụ khác nhau trên các máy. Mục đích chính của hệ thống giám sát là để phát hiện và báo cáo về bất kỳ hệ thống không hoạt động, càng sớm càng tốt. Do đó ta nhận thức được vấn đề trước khi người dùng sử dụng.

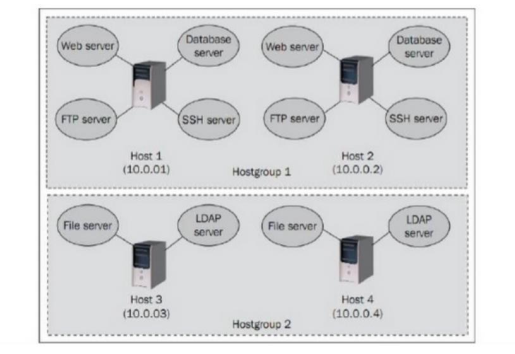
Nagios không thực hiện bất kỳ kiểm tra máy chủ hoặc các dịch vụ nào trên của máy chủ Nagios. Nó sử dụng plugin để thực hiện việc kiểm tra thực tế. Điều này làm cho nó có tính linh hoạt cao, và là giải pháp hiệu quả cho việc thực hiện và kiểm tra dịch vụ.

Nagios có hai ưu điểm lớn khi nói đến quá trình giám sát, thay vì theo dõi các giá trị, nó chỉ sử dụng bốn mức độ để mô tả tình trạng: OK, WARNING, CRITICAL và UNKNOW. Các mô tả tình trạng của các đối tượng giám sát cho phép người quản trị giải quyết hay bỏ các vấn đề trên hệ thống mà không tốn nhiều thời gian. Đây chính là điều Nagios làm. Nếu ta đang theo dõi một giá trị số như lượng không giãn và tải CPU, ta có thể định nghĩa ngưỡng những giá trị để được cảnh báo khi cần thiết.

Một thuận tiện khác của Nagios là các báo cáo về trạng thái của các dịch vụ đang hoạt động. Báo cáo này cung cấp một cái nhìn tổng quan tốt về tình trạng cơ sở hạ tầng. Nagios cũng cung cấp các báo cáo tương tự cho các nhóm máy chủ và các nhóm dịch vụ, cảnh báo khi bất kỳ dịch vụ quan trọng hoặc cơ sở dữ liệu server ngưng hoạt động. Báo cáo này cũng có thể giúp xác định độ ưu tiên của các vấn đề nào cần giải quyết trước.

Đối tượng giám sát của Nagios được chia thành hai loại: host và dịch vụ. Host là các máy vật lý (máy chủ, bộ định tuyến, máy trạm, máy in...), trong khi dịch vụ là những chức năng cụ thể.

Ví dụ: Một máy chủ web (quá trình xử lý http) có thể được định nghĩa như là một dịch vụ được giám sát. Mỗi dịch vụ có liên quan đến một máy chủ là dịch vụ đang chạy trên đó. Ngoài ra, cả hai máy và dịch vụ có thể được nhóm lại thành các nhóm cho phù hợp.



**Hình 3: Các đối tượng cần giám sát trên Nagios**

Nagios thực hiện tất cả các kiểm tra của mình bằng cách sử dụng plugins. Đây là những thành phần bên ngoài mà Nagios qua đó lấy được thông tin về những gì cần được kiểm tra và cung cấp các cảnh báo cho người quản trị. Plugins có trách nhiệm thực hiện các kiểm tra và phân tích kết quả.

Các đầu ra từ một kiểm tra đó là một trạng thái (OK, WARNING, CRITICAL và UNKNOW) và các văn bản bổ sung cung cấp thông tin về các dịch vụ cụ thể. Văn bản này chủ yếu dành cho các quản trị viên hệ thống để có thể đọc một tráng thái chỉ tiết của một dịch vụ.

Nagios không chỉ cung cấp một hệ thống cốt lõi để theo dõi, mà còn cung cấp một tập các plugins tiêu chuẩn trong một gói riêng biệt. Những plugins này cho phép kiểm tra các dịch vụ đang chạy trên hệ thống. Ngoài ra nếu ta muốn thực thi một kiểm tra đặc biệt ta có thể tạo một plugins cho riêng mình [3].

### 1.2.2 Chức năng của Nagios

Giám sát trạng thái hoạt động của các dịch vụ mạng (SMTP, POP3, IMAP, HTTP, ICMP, FTP, SSH, DHCP, LDAP, DNS, name server, web proxy, TCP port, UDP port, cơ sở dữ liệu: mysql, postgreSQL, oracle)

Giám sát các tài nguyên các máy phục vụ và các thiết bị đầu cuối (chạy hệ điều hành Unix/Linux, Windows, Novell Netware)

Giám sát các thông số an toàn thiết bị phần cứng trên host như: nhiệt độ CPU, tốc độ quạt, pin, giờ hệ thống…

Giám sát các thiết bị mạng có IP như Router, Switch và máy in. Với Router, Switch, Nagios có thể theo dõi được tình trạng hoạt động, trạng thái bật tắt của từng cổng, lưu lượng băng thông qua mỗi cổng, thời gian hoạt động liên tục (Uptime) của thiết bị. Với máy in, Nagios có thể nhận biết được nhiều trạng thái, tình huống xảy ra như kẹt giấy, hết mực...

Cảnh báo cho người quản trị bằng nhiều hình thức như email, tin nhắn tức thời (IM), âm thanh …nếu như có thiết bị, dịch vụ gặp trục trặc

Tổng hợp, lưu giữ và báo cáo định kỳ tình trạng hoạt động của mạng.

### 1.2.3 Đặc điểm Nagios

Hệ thống giám sát thu nhập và dùng dữ liệu từ các thành phần mạng cho các chức năng liên quan. Trong khi đó, mạng vẫn tiếp tục giám sát để đảm bảo vấn đề sẽ được phát hiện trước khi mạng bị sập. Việc tiếp tục công việc như vậy sẽ tích lũy một lượng dữ liệu và nó có thể làm chậm hiệu suất, tác động đến không gian lưu trữ dữ liệu hay làm chậm việc xử lý sự cố, giám sát hệ thống sử dụng dữ liệu tích hợp là để tránh những việc như việc xảy ra.

Tích hợp dữ liệu là một quá trình thu thập dữ liệu theo thời gian đã được tổng hợp và gói gọn để dữ liệu trở thành dạng chi tiết. Mức độ chi tiết của bản báo cáo được tạo ra bởi dữ liệu tích hợp sẽ phụ thuộc vào mô hình mà hệ thống được tích hợp. Dữ liệu sẽ được lấy trung bình theo thời gian và đưa vào bảng dữ liệu chi tiết, điều này giúp hệ thống giám sát tạo ra các bản báo cáo về các nút có thể kéo dài khoảng thời gian trong mạng mà không gây ra các vấn đề về hiệu suất hay không gian lưu trữ.

Các hoạt động kiểm tra được thực hiện bởi các plugin cho máy phục vụ Nagios và các mô đun client trên các thiết bị của người dùng cuối, Nagios chỉ định kỳ nhận các thông tin từ các plugin và xử lý những thông tin đó (thông báo cho người quản lý, ghi vào tệp log, hiển thị lên giao diện web...).

Thiết kế plugin đơn giản cho phép người dùng có thể tự định nghĩa và phát triển các plugin kiểm tra các dịch vụ theo nhu cầu riêng bằng các công cụ lập trình như shell scripts, C/C++, Perl, Ruby, Python, PHP, C#.

Có khả năng kiểm tra song song trạng thái hoạt động của các dịch vụ (đồng thời kiểm tra nhiều dịch vụ).

Hỗ trợ khai báo kiến trúc mạng. Nagios không có khả năng nhận dạng được topo của mạng. toàn bộ các thiết bị, dịch vụ muốn được giám sát đều phải khai báo và định nghĩa trong cấu hình.

Gửi thông báo đến người/nhóm người được chỉ định sẵn khi dịch vụ/host được giám sát gặp vấn đề và khi chúng khôi phục hoạt động bình thường (qua e-mail, pager, SMS, IM...)

Khả năng định nghĩa bộ xử lý sự kiện thực thi ngay khi có sự kiện xảy ra với host/ dịch vụ.

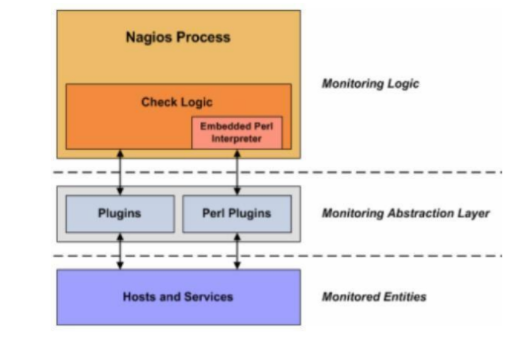
Giao diện web cho phép xem trạng thái của mạng, thông báo, history, tệp log.

### 1.2.4 Kiến trúc và tổ chức hoạt động

1. **Kiến trúc của Nagios**

**Phần lõi nagios**: có chức năng quản lý các host/dịch vụ được giám sát, thu thập các kết quả kiểm tra (check) host/dịch vụ từ các plugin gửi về, biểu diễn trên giao diện chương trình, lưu trữ và thông báo cho người quản trị.Ngoài ra nó còn tổng hợp và đưa ra các báo cáo về tình hình hoạt động chung hoặc của từng host/dịch vụ trong một khoảng thời gian nào đó.

**Plugin:** là bộ phận trực tiếp thực hiện kiểm tra host/dịch vụ. Mỗi một loại dịch vụ đều có một plugin riêng biệt được viết để phục vụ riêng cho công việc kiểm tra dịch vụ đó. Plugin là các script (Perl, C …) hay các tệp đã được biên dịch (executable). Khi cần thực hiện kiểm tra một host/dịch vụ nào đó Nagios chỉ việc gọi plugin tương ứng và nhật kết quả kiểm tra từ chúng. Với thiết kế như thế này, hệ thống Nagios rất dễ dàng được mở rộng và phát triển. Bất kì một thiết bị hay dịch vụ nào cũng có thể được giám sát nếu như viết được plugin cho nó. Hình bên dưới cho ta thấy sự tương quan giữa các thành phần trong Nagios.



**Hình 4: Sơ đồ tổ chức của Nagios**

1. **Cách thức tổ chức hoạt động**

* Kiểm tra dịch vụ trực tiếp.
* Chạy các plugin trên máy ở xa bằng secure shell.
* Bộ thực thi plugin từ xa (NRPE - Nagios Remote Plugin Executor).
* Giám sát qua SNMP.
* NSCA (Nagios Service Check Acceptor).

## Giao thức giám sát SNMP

Giao thức là một tập hợp các thủ tục mà các bên tham gia cần tuân theo để có thể giao tiếp được với nhau. Trong lĩnh vực thông tin, một giao thức quy định cấu trúc, định dạng (format) của dòng dữ liệu trao đổi với nhau và quy định trình tự, thủ tục để trao đổi dòng dữ liệu đó. Nếu một bên tham gia gửi dữ liệu không đúng định dạng hoặc không theo trình tự thì các bên khác sẽ không hiểu hoặc từ chối trao đổi thông tin. SNMP (Simple Network Management Protocol) là một giao thức, do đó nó có những quy định riêng mà các thành phần trong mạng phải tuân theo.

Một thiết bị hiểu được và hoạt động tuân theo giao thức SNMP được gọi là “có hỗ trợ SNMP” (SNMP supported) hoặc “tương thích SNMP” (SNMP compatible).

Ví dụ một số khả năng của phần mềm SNMP:

Theo dõi tốc độ đường truyền của một Router, biết được tổng số byte đã truyền/nhận.

Lấy thông tin máy chủ đang có bao nhiêu ổ cứng, mỗi ổ cứng còn trống bao nhiêu. Tự động nhận cảnh báo khi Switch có một port bị down. Điều khiển tắt (shutdown) các port trên Switch.

SNMP dùng để quản lý mạng, nghĩa là nó được thiết kế để chạy trên nền TCP/IP và quản lý các thiết bị có nối mạng TCP/IP. Các thiết bị mạng không nhất thiết phải là máy tính mà có thể là Switch, Router, firewall, adsl gateway, và cả một số phần mềm cho phép quản trị bằng SNMP.

Ví dụ: Giả sử bạn có một cái máy giặt có thể nối mạng IP và nó hỗ trợ SNMP thì bạn có thể quản lý nó từ xa bằng SNMP.

SNMP là giao thức đơn giản, do nó được thiết kế đơn giản trong cấu trúc bản tin và thủ tục hoạt động, và còn đơn giản trong bảo mật (ngoại trừ SNMP version 3). Sử dụng phần mềm SNMP, người quản trị mạng có thể quản lý, giám sát tập trung từ xa toàn mạng của mình [4].

### Ưu điểm

SNMP được thiết kế để đơn giản hóa quá trình quản lý các thành phần trong mạng. Nhờ đó các phần mềm SNMP có thể được phát triển nhanh và tốn ít chi phí.

SNMP được thiết kế để có thể mở rộng các chức năng quản lý, giám sát. Không có giới hạn rằng SNMP có thể quản lý được cái gì. Khi có một thiết bị mới với các thuộc tính, tính năng mới thì người ta có thể thiết kế “custom” SNMP để phục vụ cho riêng mình.

SNMP được thiết kế để có thể hoạt động độc lập với các kiến trúc và cơ chế của các thiết bị hỗ trợ SNMP.Các thiết bị khác nhau có hoạt động khác nhau nhưng đáp ứng SNMP là giống nhau. Ví dụ bạn có thể dùng 1 phần mềm để theo dõi dung lượng ổ cứng còn trống của các máy chủ chạy HĐH Windows và Linux; trong khi nếu không dùng SNMP mà làm trực tiếp trên các HĐH này thì bạn phải thực hiện theo các cách khác nhau.

### Nhược điểm

* Làm tăng lưu lượng đáng kể.
* Không cho phép phân bổ tác động trực tiếp cho các đại lý.
* Không có sự điều khiển tổng hợp của nhiều nơi quản lý.

### Điều hành SNMP

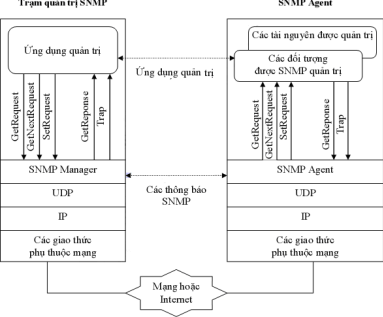
1. **Các thành phần**

Hệ thống quản lý mạng dựa trên SNMP gồm ba thành phần: bộ phận quản lý (manager), đại lý (agent) và cơ sở dữ liệu gọi là cơ sở thông tin quản lý (MIB). Mặc dù SNMP là một giao thức quản lý việc chuyển giao thông tin giữa ba thực thể trên, song nó cũng định nghĩa mối quan hệ client-server. Ở đây, những chương trình client là bộ phận quản lý, trong khi client thực hiện ở các thiết bị từ xa có thể được coi là server. Khi đó, cơ sở dữ liệu do agent SNMP quản lý là đại diện cho MIB của SNMP.

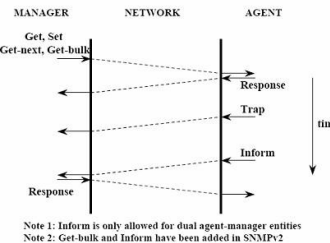
1. **Các lệnh cơ bản trong SNMP**

SNMP sử dụng 3 lệnh cơ bản là Read, Write, Trap số lệnh tùy biến để quản lý thiết bị.

* Lệnh Read: Ðược SNMP dùng để đọc thông tin từ thiết bị. Các thông tin này được cung cấp qua các biến SNMP lưu trữ trên thiết bị và được cập nhật bởi thiết bị.
* Lệnh Write: Ðược SNMP dùng để ghi các thông tin điều khiển lên thiết bị bằng cách thay đổi giá trị các biến SNMP.
* Lệnh Trap: Dùng để nhận các sự kiện gửi từ thiết bị đến SNMP. Mỗi khi có một sự kiện xảy ra trên thiết bị một lệnh Trap sẽ được gửi tới NMS.



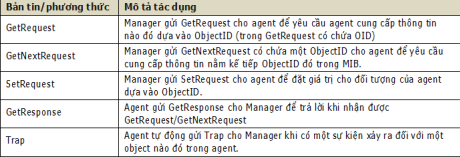
**Hình 5: Mô hình giao thức hoạt động SNMP**



**Hình 6: Hoạt động của giao thức SNMP**

### Các phương thức của SNMP

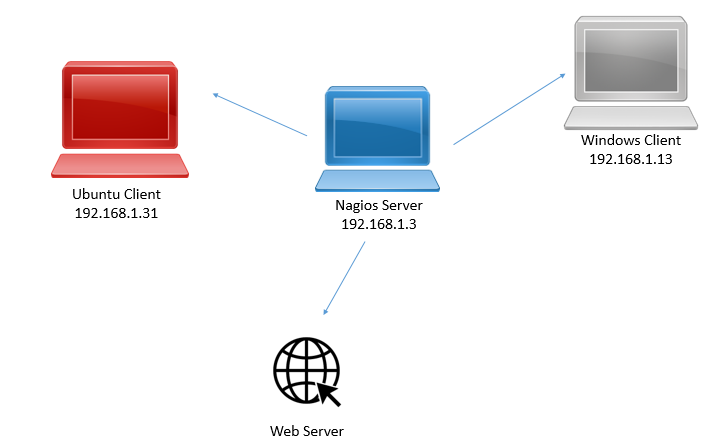
Giao thức SNMPv1 có 5 phương thức hoạt động, tương ứng với 5 loại bản tin như sau:



**Hình 7: Các phương thức cơ bản của SNMP**

# CHƯƠNG 2: THIẾT KẾ HỆ THỐNG GIÁM SÁT MẠNG BẰNG PHẦN MỀM NAGIOS

## Mô hình triển khai



**Hình 8: Mô hình triển khai giám sát Nagios**

Các thành phần hệ thống bao gồm:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Host name | IP | OS | Note |
| 1 | Nagios Server | 192.168.1.3 | Centos | Máy chủ giám sát thiết bị mạng, chương trình ứng dụng, tài nguyên các máy server khác. |
| 2 | Ubuntu | 192.168.1.31 | Ubuntu | Client các máy công ty. |
| 3 | Windows | 192.168.1.13 | Windows 7 | Client các máy công ty. |
| 4 | Website |  | www.google.com | Máy chủ dịch vụ web. |

Xây dựng kịch bản giám sát các thiết bị, máy tính của công ty và thông báo về máy chủ Nagios Server gồm:

1. Giám sát trạng thái một số host

* Trạng thái hoạt động của host.
* Trạng thái hoạt động của services.

1. Giám sát việc sử dụng tài nguyên

* CPU số lượng processes trong hàng đợi theo % sử dụng CPU của hosts.
* RAM: Cho biết dung lượng tổng và dung lượng sử dụng.
* Disk: Cho biết dung lượng tổng và đã sử dụng.

1. Cảnh báo

* Cảnh báo trạng thái: ví dụ máy Client bị down bất thường, sự cố ngoài ý muốn.
* Cảnh báo dịch vụ: Services bị tắt hay thay đổi trạng thái.

## 2.2 Giới thiệu và giải thích mô hình

Sơ đồ này giới thiệu cách thức hoạt động của hệ thống giám sát Nagios

**Vùng Internal**: Domain Controller sẽ đóng vai trò xây dựng các User- Group được sử dụng trong công ty nơi đây cũng là nơi triển khai công việc đến các máy Client. Các máy client sẽ phải đăng nhập vào Domain để lấy User sử dụng làm việc trong công ty.

**Vùng DMZ**: Vùng này chứa các server sử dụng cho công ty như Web Server (Website của công ty), FTP Server (lưu trữ các file tài liệu), Mail Server (mail nội bộ công ty). Để giám sát các máy Server chúng ta sẽ sử dụng một hệ thống giám sát Nagios.

**Vùng Internet**: cung cấp dịch vụ Internet cho người sử dụng ở công ty.

## 2.3 Cấu hình Nagios

### 2.3.1 Các tệp cấu hình chương trình

Thư mục **/usr/local/nagios/etc/**

Tệp cấu hình chính nagios.cfg. Thiết đặt những tùy chọn chung nhất của Nagios, tác động đến cách thức hoạt động của Nagios. Trong nagios.cfg bạn có thể khai báo đường dẫn các tệp cấu hình còn lại, tệp log, tệp đệm … hoặc bật tắt các tùy chọn cấu hình như cho phép thông báo, sử dụng lệnh ngoại trú, kiểm tra bị động, cách thức log, cập nhật…

Tệp cấu hình tài nguyên resource.cfg. Các tệp tài nguyên dùng để lưu trữ các nhãn (macro) được định nghĩa bởi người dùng, và lưu trữ những thông tin nhạy cảm (như mật khẩu…), ẩn với CGIs. Bạn có thể chỉ định một hay nhiều tùy chọn tệp tài nguyên bằng cách sử dụng chỉ thị resource\_file trong tệp cấu hình chính.

Tệp cấu hình CGI cgi.cfg. Tệp cấu hình CGI chứa tập các chỉ thị ảnh hưởng đến hoạt động của CGIs và cách thức hiển thị thông tin trên giao diện web.

### 2.3.2 Các tệp cấu hình đối tượng

Thư mục **/usr/local/nagios/etc/objects**

Nơi lưu trữ các tệp cấu hình đối tượng được giám sát và quản lý trong nagios. Các tệp định nghĩa đối tượng được sử dụng để định nghĩa host, dịch vụ, liên hệ (contacts), nhóm liên hệ (contact groups), lệnh… đây là nơi định nghĩa tất cả mọi thứ mà bạn muốn giám sát và cách mà bạn giám sát chúng. Bạn có thể chỉ định một hay nhiều tệp định nghĩa đối tượng bằng sử dụng các chỉ thị cfg\_file và cfg\_dir trong tệp cấu hình chính. Các tệp cấu hình sẵn có là:

* Localhost.cfg //định nghĩa các máy linux
* Contact.cfg //định nghĩa người dùng
* Printer.cfg // định nghĩa các máy in
* Switch.cfg // định nghĩa Switch
* Window.cfg // định nghĩa máy window
* Command.cfg // định nghĩa các lệnh
* Template.cfg //mẫu định nghĩa có sẵn
* Timeperiods.cfg //định nghĩa các chu kì thời gian



**Hình 9: Các tệp đối tượng**

### 2.3.3 Định nghĩa host

Host là một trong những đối tượng cơ bản nhất được giám sát. Đặc điểm của host là:

* Host thường là các thiết bị vật lý trên mạng như server, workstation, Router, Switch, Printer…
* Host có địa chỉ xác định (IP hoặc MAC).
* Host thường có ít nhất một dịch vụ liên quan đến nó.
* Một host có thể có mối quan hệ Cha/con, phụ thuộc vào host khác.

Khi định nghĩa đối tượng host bạn có thể kế thừa mẫu định nghĩa host có trong tệp template.cfg. Tuy nhiên với mỗi host được định nghĩa thì có 3 tùy chọn bắt buộc phải khai báo cho phù hợp. Đó là tên host, bí danh và địa chỉ IP của host.

define host {

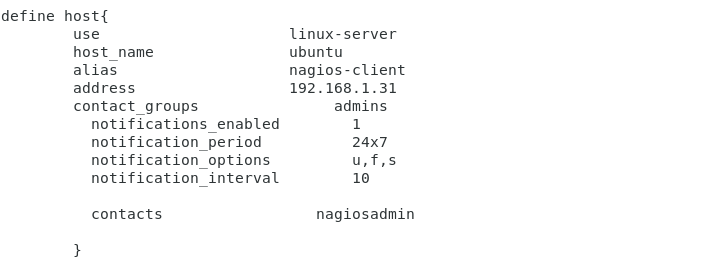
use linux-server

host\_name ubuntu

alias nagios-client

address 192.168.1.31 …

}



**Hình 10: Định nghĩa host**

### 2.3.4 Định nghĩa dịch vụ

Định nghĩa dịch vụ dùng để khai báo dịch vụ được giám sát chạy trên host. Dịch vụ ở đây có thể hiểu là các dịch vụ mạng thực sự như POP, SMTP, HTTP… hay chỉ là một số số liệu của host như số lượng người dùng, ổ đĩa còn trống… Các tùy chọn dưới đây là bắt buộc khi định nghĩa một dịch vụ mới.

define service {

host\_name linux-server service\_des

cription check-disk-sda1

check\_command check-disk!/dev/sda1

max\_check\_attempts 5

check\_interval 5

retry\_interval 3

check\_period 24x7

notification\_interval 30

notification\_period 24x7

notification\_options w, c, r

contact\_groups linux-admins

}

Tuy nhiên cũng giống như định nghĩa host, nếu sử dụng kế thuad từ định nghĩa mẫu thì khi định nghĩa một host mới chỉ cần khai báo 4 tùy chọn:

define service {

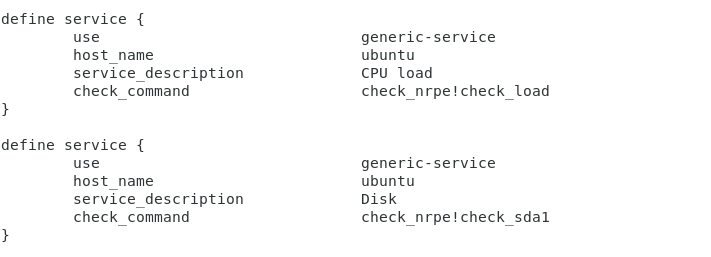
use generic-service

host\_name linux-server

service\_description check-disk-sda1

check\_command check-disk! /dev/sda1

}



**Hình 11: Định nghĩa dịch vụ**

### 2.3.5 Định nghĩa lệnh

Tất cả các hành động của Nagios như kiểm tra host/dịch vụ, thông báo, xử lý sự kiện đều được thực hiện bằng cách gọi lệnh. Tất cả các lệnh trong Nagios đều được định nghĩa trong tệp cấu hình commands.cfg.

define command {

command\_name Ten Lenh

command\_line Nguoi dung/script! Danh sach tham so

}

### Cấu hình Nagios Server

1. **Yêu cầu hệ thống**

Server: CPU duo core, RAM >= 1GB, HDD >=50GB tùy theo nhu cầu lưu lượng

OS: Windows, Linux, Unix. Ở đây ta chọn CentOS 6.10 64bit, vừa nhẹ, không quan tâm lisence và tận dụng cho các công tác hệ thống khác.

Nagios core: Hiện tại đã có bản Nagios 4.3.4, nhưng ta dùng version 4.0.8 cho server vì tính ổn định

Web: dùng Apache2 hoặc httpd

PHP, net-snmp: bản mới nhất

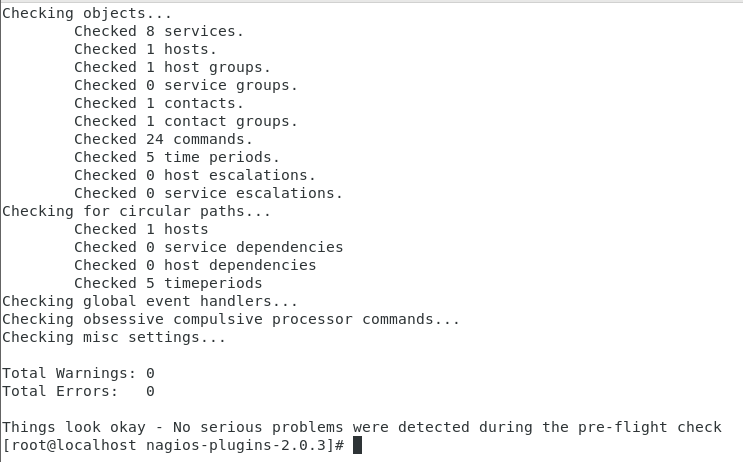
Các gói yêu cầu trước khi cài đặt Nagios: Apache, PHP, GCC compiler, GD development libraries

yum install httpd php gcc glibc glibc-common gd gd-devel

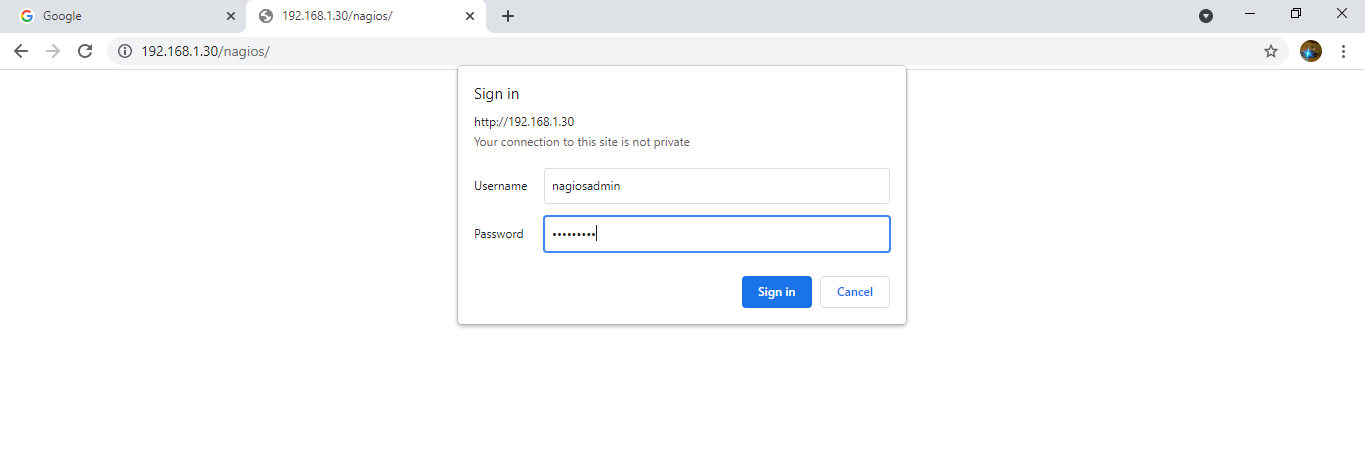
1. **Cài đặt Nagios Server:**

* Tạo thông tin tài khoản
* Tải về Nagios và Plugin
* Biên dịch và cài đặt Nagios
* Tùy chỉnh cấu hình (/usr/local/nagios/etc): thay đổi địa chỉ email trong phần nagiosadmin thành địa chỉ email của người nhận cảnh báo các nguy cơ của mạng từ Nagios.
* Cấu hình giao diện Web (thư mục conf.d của apache)
* Biên dịch và cài đặt các Nagios Plugin
* Khởi động Nagios

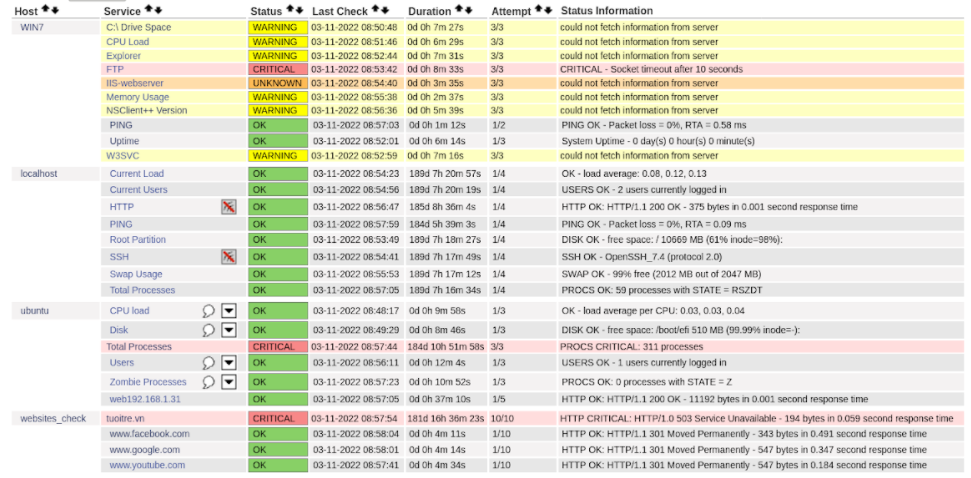
**Kết quả cài đặt:**



**Hình 12: Kiểm tra Warnings/Errors của hệ thống Nagios**



**Hình 13: Đăng nhập Nagios Server**



**Hình 14: Giao diện giám sát Nagios**

# CHƯƠNG 3: ỨNG DỤNG THỰC NGHIỆM

## Kịch bản 1: Sự cố Mail Server

1. **Giám sát dịch vụ smtp:** check\_smtp plugin được sử dụng để giám sát email server. Tệp commands.cfg chứa định nghĩa lệnh sử dụng check\_smtp plugin:

define command {

command\_name check\_smtp

command\_line $USER1$/check\_smtp –H $HOSTADDRESS $ARG1$

}

Dưới dây là định nghĩa dịch vụ đơn giản cho việc giám sát SMTP server:

define service {

use generic-service

host name remotehost

service\_description SMTP Response Check

check\_command check\_smtp

}

Định nghĩa dịch vụ này sẽ giám sát dịch vụ SMTP server và tạo ra thông báo nếu SMTP server không trả lời sau 10 giây.

Còn định nghĩa dưới đây sẽ kiểm tra SMTP server và tạo ra thông báo nếu SMTP server không trả lời sau 5 giây và thông điệp trả về không chứa đoạn “mailtestserver.com”

define service {

use generic-service

host name remotehost

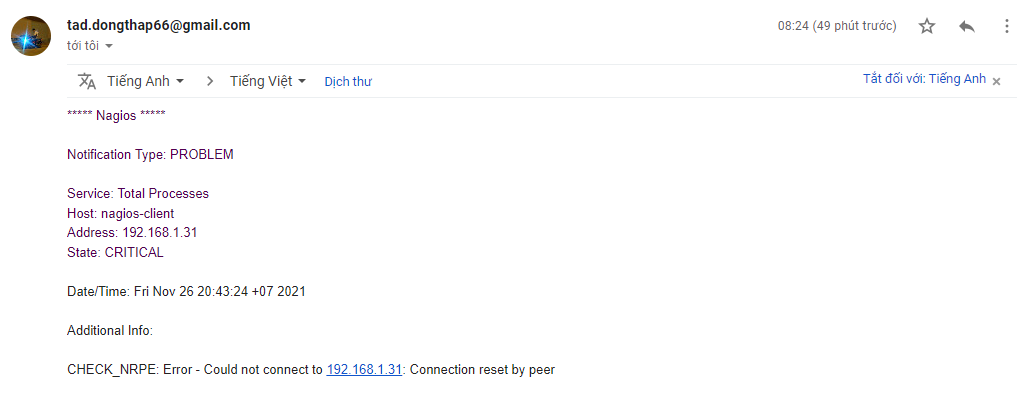
service\_description SMTP Response Check

check\_command check\_smtp! -t 5 –e “mailtestserver.com”

}

1. **Tiến hành xây dựng kịch bản sự cố**

Mặc định, dịch vụ đang chạy tốt, chúng ta tiến hành tắt dịch vụ. Hệ thống Nagios sẽ nhận thấy bất thường xảy ra với dịch vụ SMTP server đang được giám sát, hệ thống sẽ gửi về thông điệp cảnh báo Mail Server đã tạm thời ngừng hoạt động do lỗi kỹ thuật hoặc lý do đột ngột nào đó để người quản trị có thể nhanh chóng kiểm tra và khắc phục sự cố để hệ thống giám sát hoạt động bình thường.



**Hình 15: Cảnh báo Mail Server**

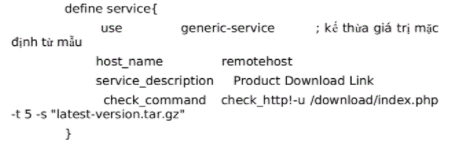
## Kịch bản 2: Sự cố Web Server

1. **Giám sát http:** Nagios sử dụng plugin check\_http trong việc giám sát dịch vụ HTTP trên web server. Check\_http có thể nhận biết được các thông tin sau:

* Thời gian trả lời của web server
* Mã lỗi tả về của dịch vụ http (403: không tìm thấy tệp; 404: lỗi xác thực)
* Nội dung chuỗi trả về có chứa chuỗi s cho trước không
* Một URL nào đó có còn nằm trên web server hay không

Để giám sát ở mức sâu hơn bạn có thể xem hướng dẫn check\_http plugin với tham số dòng lệnh là –help. Cú pháp –help có ở tất cả các plugin.

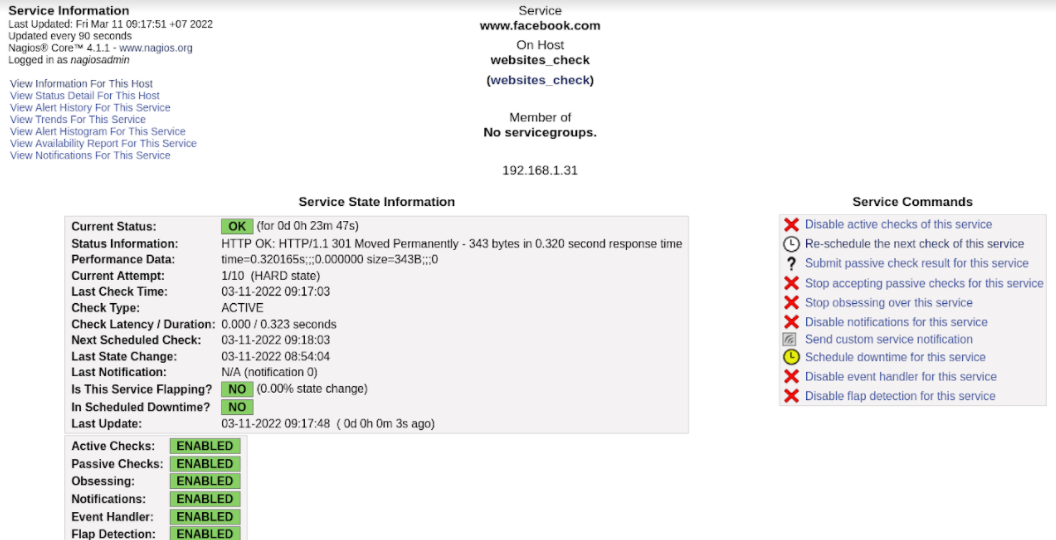
Dưới đây là một định nghĩa dịch vụ ở mức sâu hơn. Nó kiểm tra xem download/index.php URL có chứa chuỗi “latest-version.tar.gz” hay không. Thông báo lỗi nếu không tìm thấy, URI không hợp lệ, hay là web server trả lời sau 5 giây.



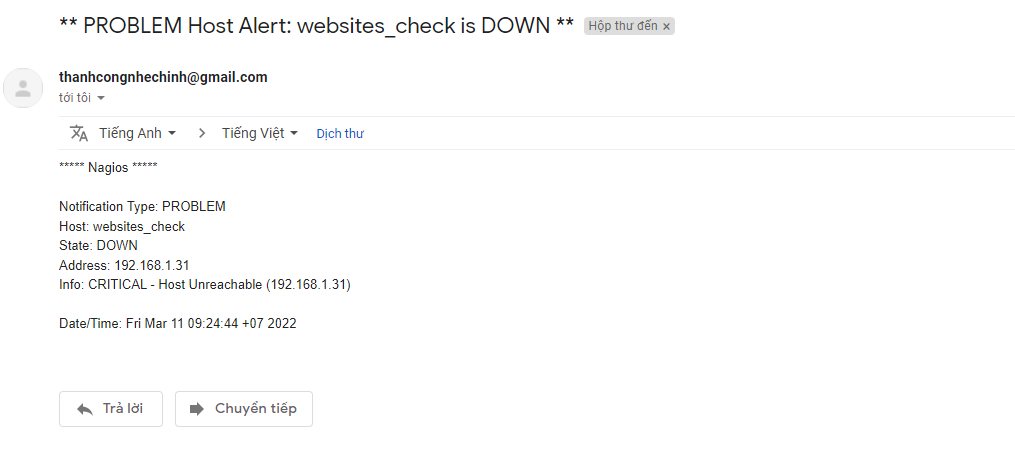
**Hình 16: Service check http**

1. **Xây dựng kịch bản sự cố**

Mặc định, dịch vụ đang chạy tốt, chúng ta tiến hành tắt dịch vụ. Hệ thống Nagios sẽ nhận thấy bất thường xảy ra với dịch vụ HTTP đang được giám sát, hệ thống sẽ gửi về thông điệp cảnh báo Web Server đã tạm thời ngừng hoạt động do lỗi kỹ thuật hoặc lý do đột ngột nào đó để người quản trị có thể nhanh chóng kiểm tra và khắc phục sự cố để hệ thống giám sát hoạt động bình thường.



**Hình 17: Xây dựng kịch bản sự cố Web Server**



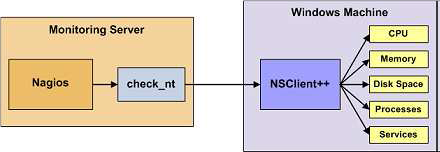
**Hình 18: Nagios báo cáo cảnh báo sự cố Web**

## Kịch bản 3: Sự cố với Client

1. **Giám sát máy chạy hệ điều hành Windows:**

Nagios có thể giám sát các dịch vụ và thuộc tính của máy chạy hệ điều hành Windows như là:

* Sử dụng bộ nhớ
* Tình trạng CPU
* Sử dụng ổ đĩa
* Trạng thái các dịch vụ
* Các tiến trình đang chạy
* …



**Hình 19: Giám sát máy chạy hệ điều hành Windows**

Để giám sát các dịch vụ hoặc các thuộc tính trên máy Windows thì ta cần cài các agent lên chúng. Agent này hoạt động như một proxy giữa Nagios Plugins với các dịch vụ hoặc các thuộc tính cần giám sát của máy Windows.

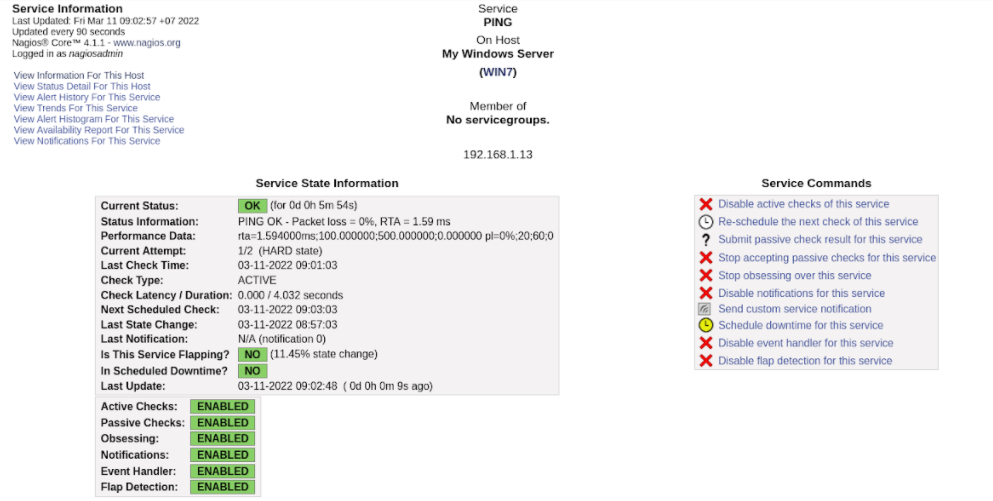
Ví dụ trên chúng ta sẽ cài đặt NSClient++ trên máy Windows, sử dụng check\_nt plugin để giao tiếp với NSClient++. Check\_nt plugins được cài đặt trên máy Nagios Server. Để giám sát các host Windows, chúng ta có thể sử dụng trực tiếp thông qua giao thức SNMP để thu thập thông tin từ máy Windows.

Các bước giám sát một máy Windows mới là:

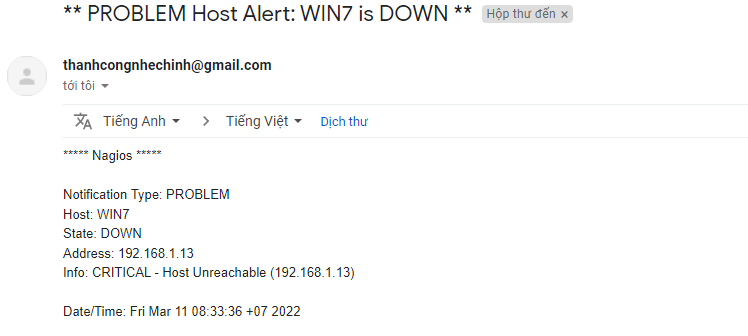
* Thực hiện các yêu cầu ban đầu
* Cài đặt nột agent giám sát trên Windows
* Tạo một host mới và xác định các dịch vụ cần thiết được giám sát trên máy Windows
* Khởi động lại Nagios

1. **Tiến hành xây dựng sự cố Client**

Mặc định, dịch vụ đang chạy tốt, chúng ta tiến hành tắt một dịch vụ bất kỳ (ví dụ: CPU, Disk Space,...). Hệ thống Nagios sẽ nhận thấy bất thường xảy ra với dịch vụ của Client đang được giám sát, hệ thống sẽ gửi về thông điệp cảnh báo về dịch vụ đã tạm thời ngừng hoạt động do lỗi kỹ thuật hoặc lý do đột ngột nào đó để người quản trị có thể nhanh chóng kiểm tra và khắc phục sự cố để hệ thống giám sát hoạt động bình thường.



**Hình 20: Xây dựng kịch bản sự cố Client**



**Hình 21: Nagios báo cáo cảnh báo sự cố Client**

## 3.4 Nhận định kết quả

Nagios ở trạng thái UP 100% trong thời gian được giám sát. Ta có thể thấy được rằng tuy là một hệ thống nguồn mở nhưng Nagios hoạt động rất ổn định. Phát hiện chính xác các thay đổi của các dịch vụ mạng. Thứ nữa do thiết kế theo kiểu plugin nên Nagios rất uyển chuyển trong việc giám sát. Người dùng có thể tự viết script thực thi việc giám sát các dịch vụ theo ý mình. Hầu như tất cả các dịch vụ, thiết bị mạng đều có thể viết được plugin giám sát. Tuy nhiên việc cài đặt, cấu hình Nagios còn rườm rà và mất khá nhiều thời gian và công sức.

# KẾT LUẬN

Trong đồ án này đã nghiên cứu, tìm hiểu xây dựng hệ thống giám sát mạng dựa trên phần mềm nguồn mở Nagios.

Đã áp dụng các kiến thức của các môn học như quản trị mạng, mạng máy tính ... vào mô hình và thực tế. Đã học hỏi được thêm nhiều kinh nghiệm về cách thức tổ chức, xây dựng hệ thống giám sát cũng như quy hoạch hệ thống. Tuy nhiên, do thời gian và khả năng có hạn, nên chưa đi sâu tìm hiểu được thêm những vấn đề cần thiết của hệ thống. Mô hình giám sát hệ thống mạng Nagios mới chỉ dừng ở mức độ theo dõi, giám sát máy chủ như giám sát tài nguyên máy, dung lượng traffic, tình trạng của host.

Trong tương lai sự phát triển và nghiên cứu sâu hơn về hệ thống giám sát mạng Nagios và các công cụ hỗ trợ giám sát mạng, giám sát sâu hơn những vấn đề cần thiết của hệ thống sẽ được tiếp tục. Phát triển các chức năng trên Nagios như: giám sát hạ tầng mạng bao gồm các thiết bị Router, Switch, Firewall... Cảnh báo qua SMS.

# TÀI LIỆU THAM KHẢO

1. <https://en.wikipedia.org/wiki/Nagios>
2. <https://adminvietnam.org/nagios-tren-centos-6/121/>
3. <https://www.nagios.com>
4. Essential SNMP / Douglas R. Mauro and Kevin J. Schmidt.
5. SNMP toàn tập – Nguyễn Thanh Diệp

|  |  |
| --- | --- |
|  | TP. HCM, ngày 13 tháng 03 năm 2022 |
|  | **XÁC NHẬN CỦA GIẢNG VIÊN HƯỚNG DẪN** |
|  | **ThS. HUỲNH THANH TÂM TS. HUỲNH TRỌNG THƯA** |