BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG
-------o0o-------

SỬ DỤNG PHẦN MỀM NAGIOS ĐỂ GIÁM SÁT HỆ THỐNG MẠNG

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ Thông tin

HẢI PHÒNG - 2020

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG
-------o0o-------

SỬ DỤNG PHẦN MỀM NAGIOS ĐỂ GIÁM SÁT HỆ THỐNG MẠNG

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

Ngành: Công nghệ Thông tin

Sinh viên thực hiện : **Phạm Quang Anh**
Mã sinh viên : **1412102013**
Giáo viên hướng dẫn : **TS. Ngô Trường Giang**.

HẢI PHÒNG - 2020

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

-------o0o-------

NHIỆM VỤ THIẾT KẾ TỐT NGHIỆP

Sinh viên: **Phạm Quang Anh** Mã sinh viên: **1412102013**

Lớp: **CT1901M** Ngành: **Công nghệ Thông tin**

Tên đề tài:

"SỬ DỤNG PHẦN MỀM NAGIOS ĐỂ GIÁM SÁT HỆ THỐNG MẠNG"

NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp

a. Nội dung:

- Tổng quan về giám sát hệ thống mạng.
- Giao thức trong giám sát hệ thống mạng.
- Phần mềm giám sát mạng nagios.

b. Các yêu cầu cần giải quyết

- Tìm hiểu các vấn đề cơ bản về giám sát hệ thống mạng.
- Tìm hiểu các giao thức giám sát mạng
- Cài đặt, cấu hình phần mềm nagios để giám sát hệ thống mạng.

2. Các số liệu cần thiết để thiết kế, tính toán

3. Địa điểm thực tập

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Người hướng dẫn thứ nhất:

Họ và tên: **Ngô Trường Giang**

Học hàm, học vị: **Tiến sĩ.**

Cơ quan công tác: **Khoa Công nghệ Thông tin**

Nội dung hướng dẫn:

- Tổng quan về giám sát hệ thống mạng.
- Giao thức trong giám sát hệ thống mạng.
- Phần mềm giám sát mạng nagios.

Người hướng dẫn thứ hai:

Họ và tên: …….....

Học hàm, học vị……

Cơ quan công tác: ……

Nội dung hướng dẫn: …….....

……..

……..

Đề tài tốt nghiệp đ□ợc giao ngày 14 tháng 10 năm 2019.

Yêu cầu phải hoàn thành tr□ớc ngày 10 tháng 01 năm 2020.

Đã nhận nhiệm vụ: Đ.T.T.N Sinh viên	Đã nhận nhiệm vụ: Đ.T.T.N Cán bộ hướng dẫn Đ.T.T.N
Phạm Quang Anh	**Ngô Trường Giang**

Hải Phòng, ngày .....tháng.....năm 2020

HIỆU TRƯỞNG

GS.TS.NGUT Trần Hữu Nghị

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập – Tự do – Hạnh phúc

PHIẾU NHẬN XÉT CỦA CÁN BỘ HƯỚNG DẪN TỐT NGHIỆP

Họ và tên: **Ngô Trường Giang**

Cơ quan công tác: **Khoa Công nghệ Thông tin**

Họ tên sinh viên: **Phạm Quang Anh**

Ngành: **Công nghệ Thông tin**

Nội dung hướng dẫn:

- Tổng quan về giám sát hệ thống mạng.
- Giao thức trong giám sát hệ thống mạng.
- Phần mềm giám sát mạng nagios.

1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp:

- Sinh viên tích cực, chủ động tìm đọc các tài liệu liên quan tới đề tài
- Chấp hành nghiêm túc kế hoạch, tiến độ đề ra.

2. Đánh giá chất lượng của đồ án (so với nội dung yêu cầu đã đề ra trong nhiệm vụ đề tài tốt nghiệp trên các mặt lý luận, thực tiễn, tính toán số liệu..):

- Về mặt lý thuyết: Đồ án đã trình bày tổng quan về giám sát hệ thống mạng, giao thức giám sát mạng, các chức năng cơ bản của phần mềm nagios.
- Về mặt thực nghiệm: Đồ án đã triển khai cài đặt, cấu hình phần mềm nagios, triển khai thử nghiệm một số giải pháp giám sát hệ thống mạng trên nagios.
- Về hình thức: Báo cáo trình bày sáng sủa, bố cục hợp lý.
- Đồ án đáp ứng được yêu cầu đề ra.

3. Ý kiến của cán bộ hướng dẫn:

Đạt [x] Không đạt [ ] Điểm:……...

Ngày 01 tháng 01 năm 2020

Cán bộ hướng dẫn

TS. Ngô Trường Giang

MỤC LỤC

DANH MỤC HÌNH VẼ

LỜI CẢM ƠN

Đề tài "Sử dụng phần mềm Nagios để giám sát hệ thống mạng" là nội dung Em chọn để nghiên cứu và làm đồ án tốt nghiệp sau bốn năm học chương trình đại học ngành công nghệ thông tin tại trường Đại Học Dân Lập Hải Phòng.

Để hoàn thành quá trình nghiên cứu và hoàn thiện đồ án tốt nghiệp này, lời đầu tiên Em xin gửi lời cảm ơn chân thành cảm ơn tới toàn thể quý Thầy Cô, bạn bè của Trường Đại Học Dân Lập Hải Phòng.

Bày tỏ lòng biết ơn sâu sắc nhất 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. Ngô Trường Giang cùng với tri thức và tâm huyết của Thầy đã tạo điều kiện em hoàn thành đồ án tốt nghiệp tại trường.

Cuối cùng, Em xin cảm ơn những người thân, bạn bè đã luôn bên Em, động viên, sẻ chia, giúp đỡ, cổ vũ tinh thần… Đó là nguồn động lực giúp Em hoàn thành chương trình học và đồ án tốt nghiệp này.

Hải Phòng, ngày 26 tháng 12 năm 2019

Sinh viên

Phạm Quang Anh

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.

Quản trị mạng theo giao thức SNMP là phương pháp được sử dụng rộng rãi nhất. Đây là giao thức quản lý mạng đơn giản, cung cấp khả năng giám sát và điều khiển các thiết bị mạng. Với ưn điểm cài đặt khá đơn giản, khả năng mềm dẻo trong việc mở rộng, SNMP trở thành một giải pháp hiệu quả cho việc quản lý thiết bị nhiều nhà cung cấp.

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 đươc 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 em sẽ đi sâu tìm hiểu về “Hệ thống giám sát mạng Nagios”.

CHƯƠNG 1: TỔNG QUAN GIÁM SÁT HỆ THỐNG MẠNG

1.1 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 được tình hình "sức khỏe" 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 mang 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.

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 ngưng 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 và tại sao?

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 dung trạng thái hệ thống mà ta phải biết và lý do tại sao:

Cần giám sát gì	Tại sao
Tính sẵn sàng của thiệt 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.

Khi một hệ thống mạng được triển khai và đưa vào vận hành, vấn đề giám sát hoạt động của toàn bộ hệ thống có vai trò quan trọng. Các bất thường liên quan đến thiết bị, dịch vụ, tấn công mạng, hay tài nguyên hệ thống… cần được phát hiện nhanh chóng để có giải pháp sửa chữa, thay thế, phản ứng kịp thời giúp hệ thống mạng hoạt động ổn định, thông suốt.

Trong các hệ thống mạng lớn và phức tạp như hiện nay, các thiết bị, kết nối, dịch vụ, ứng dụng đều được thiết kế mang tính dự phòng cao để sẵn sàng giải quyết khi sự cố xảy ra. Việc phát hiện kịp thời các thiết bị, các kết nối hư hỏng để tiến hành sửa chữa, thay thế lại càng cấp thiết. Vì khi sự hư hỏng xảy ra một phần, thàn phần dự phòng vẫn hoạt động. Nếu thành phần hư hỏng không được phát hiện, xử lý kịp thời sẽ có nguy cơ cao cho hoạt động của hệ thống. Nếu không có công cụ hỗ trợ, người quản trị sẽ bị động trước các tình huống bất thường xảy ra.

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: giải pháp giám sát hệ thống cho phép được thông báo tình trạng hoạt động cũng như tài nguyên của hệ thống. Nếu không có những chức năng này ta phải đợi đến khi người dùng thông báo.

Lên kế hoạch cho việc nâng cấp, sủa chữa: nếu một thiết bị ngưng hoạt động một cách thường xuyên hay băng thông mạng gần chạm tới ngưỡng thì lúc này cần phải có sự thay đổi trong hệ thống. Hệ thống giám sát mạng cho phép ta biết được những thông tin này để có thể có những đổi khi cần thiết.

Chuẩn đoán các vấn đề một cách nhanh chóng: giả sử máy chủ của ta không kết nối tới được. Nếu không có hệ thống giám sát ta không thể biết được nguyên nhân từ đâu, máy chủ hay Router hay cũng có thể là Switch. Nếu biết được chính xác vấn đề ta có thể giải quyết một cách nhanh chóng.

Xem xét những gì đang hoạt động: các báo cáo bằng đồ họa có thể giải thích tình trạng hoạt động của hệ thống. Đó là những công cụ rất tiện lợi phục vụ cho quá trình giám sát.

Biết được khi nào cần áp dụng các giải pháp sao lưu phục hồi: với đủ các cảnh báo cần thiết ta nên sao lưu dữ liệu của hệ thống phòng trường hợp hệ thống có thể bị hư hại bất kì lúc nào. Nếu không có hệ thống giám sát ta không thể biết có vấn đề xảy ra khi đã quá trễ.

Đảm bảo hệ thống bảo mật hoạt động tốt: các tổ chức tốn rất nhiều tiền cho hệ thống bảo mật. Nếu không có hệ thống giám sát ta không thể biết hệ thống bảo mật của ta có hoạt động như mong đợi hay không.

Theo dõi hoạt động của các tài nguyên dịch vụ trên hệ thống: hệ thống giám sát có thể cung cấp thông tin tình trạng các dịch vụ trên hệ thống, đảm báo người dùng có thể kết nối đến nguồn dữ liệu.

Được thông báo về tình trạng của hệ thống ở khắp mọi nơi: rất nhiều các ứng dụng giám sát cung cấp khả năng giám sát và thông báo từ xa chỉ cần có kết nối Internet.

Đảm bảo hệ thống hoạt động liên tục: nếu tổ chức của ta phụ thuộc nhiều vào hệ thống mạng, thì tốt nhất là người quản trị cần phải biết và xử lý các vấn đề trước khi sự cố nghiêm trọng xảy ra.

Tiết kiệm tiền: với tất cả các lý do ở trên, ta có thể giảm thiểu tối đa với thời gian hệ thống ngưng hoạt động, làm ảnh hưởng tới lợi nhuận của tổ chức và tiết kiệm tiền cho việc điều tra khi có sự cố xảy ra.

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: Đảm bảo các thông tin không bị lộ ra ngoài. Là một trong những phần quan trọng giữa các giám sát mạng, tính năng này sẽ theo dõi những biến động trong hệ thống mạng và cảnh báo cho quản trị viên biết khi có sự cô xảy ra kịp thời. Thông qua màn hình giám sát, người quản trị có thể xác định được vấn đề khả nghi và tìm cách giải quyết phù hợp nhất cho vấn đề đó.

Khả năng xử lý sự cố: Khả năng này một trong các lợi thế của giám sát mạng. Tiết kiệm thời gian chuẩn đoán sai lệch trong mạng, giám sát viên có thể biết chính xác thiết bị nào đang có vấn đề và xử lý nó một cách nhanh nhất trước khi dùng mạng phát hiện.

Tiết kiệm thời gian và tiền bạc: Nếu không có phần mềm giám sát thì sẽ mất nhiều thời gian để tìm kiếm và sửa lỗi hệ thống mà lẽ ra chỉ mất vài giây để sửa lỗi đó. Điều này không chỉ tốn thêm chi phí mà còn làm giảm năng suất lao động. Ngược lại, nhờ có phần mềm giám sát, vấn đề sẽ nhanh chóng tìm ra và xử lý hiệu quả, có thể tập trung nhiền hơn vào công việc khác, lợi nhuận công ty cũng gia tăng.

Lập kế hoạch thay đổi: Với giám sát mạng, giám sát viên có thể theo dõi được thiết bị nào sắp hỏng và cần phải thay mới. Giám sát mạng cho người giám sát khả năng lên kế hoạch sẵn và dễ dàng tạo ra thay đổi cần thiết cho hệ thống mạng.

1.2 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.

1.3 Các quy tắc khi thiết kế hệ thống giám sát mạng

1.3.1 Mô hình FCAPS

Một trong những quy tắc khi thiết kệ hệ thống giám sát là tuân theo mô hình FCAPS (Fault Configuration Accounting Performance Security). “Theo tiêu chuẩn của ISO (International Standard Organization), mô hình được phân loại thành 5 chức năng chính, đó là chức năng quản lý lỗi (Fault management), quản lý cấu hình (Configuratinon management), quản lý kế toán (Accounting management), quản lý hiệu năng (Performance management) và quản lý bảo mật (Security management)” [1].

Quản lý lỗi: Hạng mục này có thể thực hiện quá trình ghi nhận, cô lập và xử lý lỗi xảy ra trên mạng. Việc xác định những vấn đề tiềm ẩn trong mạng cũng do hạng mục này đảm nhiệm.

Quản lý cấu hình: Giúp thu thập và lưu trữ các cấu hình của vô số thiết bị, bao gồm việc lần ra những thay đổi cấu hình trên thiết bị, góp phần quan trọng trong việc chủ động quản trị và giám sát mạng.

Quản lý kế toán: Thường áp dụng cho các nhà cung cấp dịch vụ mạng. Trong hệ thống mạng, công việc này được thay bằng việc quản lý người dùng mạng, nói cách khác, quản trị viên sẽ cấp cho người dùng mật khẩu, quyền để vào mạng.

Quản lý hiệu năng: Quản lý toàn bộ hiệu năng của mạng, tốc độ truyền thông, lượng truyền, những gói tin bị mất, thời gian phản hồi, v.v. và thường sử dụng bằng giao thức SNMP.

Quản lý bảo mật: Là một hoạt động rất quan trọng trong quản trị mạng. Quản lý bảo mật trong FCAPS bao gồm quá trình kiểm soát truy cập tài nguyên trên mạng, kèm theo các dữ liệu, cấu hình và bảo vệ thông tin người dùng.

1.3.2 Báo cáo và cảnh cáo

Công việc của giám sát mạng là thu nhập dữ liệu từ các thành phần mạng và xử lý trình bày chúng dưới dạng mà quản trị viên có thể hiểu – tiến trình này được gọi là báo cáo. Báo cáo giúp quản trị viên biết được hiệu suất của các nút mạng, trạng thái mạng hiện tại. Với các dữ liệu từ bản báo cáo, quản trị viên có thể đưa ra quyết định về việc quản lý dung lượng, bảo trì mạng, xử lý sự cố hay bảo mật mạng.

Tuy nhiên, việc làm này không giúp quản trị viên bảo trì mạng ở hiệu suất cao. Vì thế, việc tạo các cảnh báo dựa trên ngưỡng cùng các điểm kích hoạt sẽ là nhân tố bổ sung giúp các nhà quản trị xác định các vấn đề có thể xảy ra trước khi nó gãy sụp đổ hoàn toàn hệ thống.

1.3.3 Tích hợp lưu trữ dữ liệu

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.

1.4 Các giải pháp và công cụ giám sát mạng phổ biến

Hệ thống giám sát mạng có thể được xây dựng theo một trong ba giải pháp sau:

- Giải pháp quản lý sự kiện an ninh: tập trung xử lý, phân tích các nhật ký đã được thu nhập để đưa ra cảnh báo cho người sử dụng.
- Giải pháp quản lý thông tin an ninh: tập trung thu nhập, lưu trữ và biểu diễn nhật ký.
- Giải pháp quản lý và phân tích sự kiện an ninh: là sự kết hợp của hai giáp trên nhằm khắc phục những hạn chế vốn có.

Mô hình của giải pháp quản lý và phân tích sự kiện an ninh gồm các thành phần chính [1]:

a) Thu thập nhật ký an toàn mạng bao gồm các giao diện thu thập nhật ký trực tiếp từ các thiết bị, ứng dụng và dịch vụ. Thành phần này có tính năng:

- Thu thập toàn bộ dữ liệu toàn bộ nhật ký từ các nguồn thiết bị, ứng dụng.
- Kiểm soát băng thông và không gian lưu trữ thông qua khả năng lưu trữ và chọn lọc dữ liệu nhật ký.
- Phân tách từng sự kiện và chuẩn hóa các sự kiện vào một lược đồ chung.
- Tích hợp các sự kiện để giảm thiểu số lượng các sự kiện gửi về thành phần phân tích lưu trữ.

- Chuyển toàn bộ các sự kiện đã thu thập về thanh phần phân tích và lưu trữ.

b) Thành phần phân tích và lưu trữ bao gồm các thiết bị lưu trữ dung lượng lớn, cung cấp khả năng tổng hợp và phân tích tự động. Tính năng:

- Kết nối với các thành phần thu thập nhật ký để tập hợp nhật ký tập trung và tiến hành phân tích, so sánh tương quan.
- Module phân tích sẽ được hỗ trợ bởi các luật (định nghĩa trước) cũng như khả năng tùy biến, nhằm đưa ra kết quả phân tích chính xác nhất.
- Các nhật ký an toàn mạng được tiến hành phân tích, so sánh tương quan theo thời gian thực nhằm đưa ra cảnh báo tức thời cho người quản trị.
- Hỗ trợ kết nối đến các hệ thống lưu trữ dữ liệu.

c) Thành phần quản trị mạng tập trung:

- Cung cấp giao diện quản trị tập trung cho toàn bộ hệ thống giám sát an toàn mạng.
- Hỗ trợ sẵn sàng hàng nghìn mẫu báo cáo, các giao diện theo dõi, điều kiện lọc.
- Hỗ trợ các công cụ cho việc xử lý các sự kiện an toàn mạng xảy ra trong hệ thống.

d) Các thành phần khác:

Gồm các thành phần cảnh báo, hệ thống DashBoard theo dõi thông tin, các báo cáo đáp ứng tiêu chuẩn quản lý hoặc thành phần lưu trữ dữ liệu lâu dài.

1.5 Giao thức giám sát mạng 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 compartible).

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 [5].

1.5.1.1 Ưu điểm trong thiết kế của SNMP

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.

1.5.1.2 Nhược điểm của SNMP.

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.

1.5.1.3 Các phiên bản của SNMP

SNMP có 4 phiên bản: SNMPv1, SNMPv2c, SNMPv2u và SNMPv3. Các phiên bản này khác nhau một chút ở định dạng bản tin và phương thức hoạt động. Hiện tại SNMPv1 là phổ biến nhất do có nhiều thiết bị tương thích nhất và có nhiều phần mềm hỗ trợ nhất. Trong khi đó chỉ có một số thiết bị và phần mềm hỗ trợ SNMPv3.

Năm 1993, SNMP Version 2 (SNMPv2) được IETF đưa ra với mục đích giải quyết vấn đề tồn tại trong SNMPv1 là cơ chế đảm bảo bảo mật. SNMPv2 có nhiều thay đổi so với SNMPv1 như hỗ trợ các mạng trung tâm cấp cao, mạng phân tán, cơ chế bảo mật, làm việc với khối dữ liệu lớn... Tuy

nhiên SNMPv2 không được chấp nhận hoàn toàn bởi vì SNMPv2 chưa thoả mãn vấn đề bảo mật và quản trị bởi vậy năm 1996 những phần bảo mật trong SNMPv2 bị bỏ qua và SNMPv2 được gọi là "SNMPv2 trên cơ sở truyền thông" hay SNMPv2c.

Năm 1998, IETF bắt đầu đưa ra SNMPv3 được định nghĩa trong RFCs 2571-2575. Về bản chất, SNMPv3 mở rộng để đạt được cả hai mục đích là bảo mật và quản trị. SNMPv3 hổ trợ kiến trúc theo kiểu module để có thể dễ dàng mở rộng. Như thế nếu các giao thức bảo mật được mở rộng chúng có thể được hổ trợ bởi SNMPv3 bằng cách định nghĩa như là các module riêng.

1.5.2 Điều hành SNMP

1.5.2.1 Các thành phần trong SNMP

Hệ thống quản lý mang dựa trên SNMP gồm ba thành phần: bộ phận quản lí(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 MIP của SNMP.

1.5.2.2 Bộ phận quản lý (manager)

Bộ phận quản lý là một chương trình vận hành trên một hoặc nhiều máy tính trạm. Tùy thuộc vào cấu hình, mỗi bộ phận quản lí có thể được dùng để quản lý một mạng con, hoặc nhiều bộ phận quản lý có thể được dùng để quản lý cùng một mạng con hay một mạng chung. Tương tác thực sự giữa một người sử dụng cuối (end-user) và bộ phận quản lý được duy trì qua việc sử dụng một hoặc nhiều chương trình ứng dụng mà cùng với bộ phận quản lý, biến mặt bằng phần cứng thành Trạm quản lý mạng (NMS). Ngày nay, trong thời kỳ các chương trình giao diện người sử dụng đồ họa (GUI), hầu hết những chương trình ứng dụng cung cấp môi trường cửa sổ chỉ và click chuột,

thực hiện vận hành với bộ phận quản lý để tạo ra những bản đồ họa và biểu đồ cung cấp những tổng kết hoạt động của mạng dưới dạng thấy được.

Qua bộ phận quản lý, những yêu cầu được chuyển tới một hoặc nhiều thiết bị chịu sự quản lý. Ban đầu SNMP được phát triển để sử dụng trên mạng TCP/IP và những mạng này tiếp tục làm mạng vận chuyển cho phần lớn các sản phẩm quản lý mạng dựa trên SNMP. Tuy nhiên SNMP cũng có thể được chuyển qua NetWare IPX và những cơ cấu vận chuyển khác.

1.5.2.3 Agent

Thiết bị chịu sự quản lý (Managed device): Là một nút mạng hỗ trợ giao thức SNMP và thuộc về mạng bị quản lý. Thiết bị có nhiệm vụ thu thập thông tin quản lý và lưu trữ để phục vụ cho hệ thống quản lý mạng. Những thiết bị chịu sự quản lý, đôi khi được gọi là những phần tử mạng, có thể là những bộ định tuyến và máy chủ truy cập-Access Server, Switch và bridge, hub, máy tính hay là những máy in trong mạng.

Mỗi thiết bị chịu sự quản lý bao gồm phần mềm hoặc phần sụn (firmware) dưới dạng mã phiên dịch những yêu cầu SNMP và đáp ứng của những yêu cầu đó. Phần mềm hoặc phần sụn này được coi là một agent. Mặc dù mỗi thiết bị bắt buộc bao gồm một agent chịu quản lý trực tiếp, những thiết bị tương thích không theo SNMP cũng có thể quản lý được nếu như chúng hỗ trợ một giao thức quản lý độc quyền. Để thực hiện được điều này, phải giành được một agent ủy nhiệm (proxy agent). Proxy agent này có thể được xét như một bộ chuyển đổi giao thức vì nó phiên dịch những yêu cầu SNMP thành giao thức quản lý độc quyền của thiết bị không hoạt động theo giao thức SNMP.

Mặc dù SNMP chủ yếu là giao thức đáp ứng thăm dò (poll-respond) với những yêu cầu do bộ phận quản lý tạo ra dẫn đến những đáp ứng trong agent, agent cũng có khả năng đề xướng ra một "đáp ứng tự nguyện". Đáp ứng tự nguyện này là điều kiện cảnh báo từ việc giám sát agent với hoạt động

đã được định nghĩa trước và chỉ ra rằng đã tới ngưỡng định trước. Dưới sự điều khiển của SNMP, việc truyền cảnh báo này được coi là cái bẫy (trap).

1.5.2.4 Cơ sở thông tin quản lý – MIB

Mỗi thiết bị chịu sự quản lý có thể có cấu hình, trạng thái và thông tin thống kê rất đa dạng, định nghĩa chức năng và khả năng vận hành của thiết bị. Thông tin này có thể bao gồm việc thiết lập chuyển mạch phần cứng, những giá trị khác nhau lưu trữ trong các bảng ghi nhớ dữ liệu, bộ hồ sơ hoặc các trường thông tin trong hồ sơ lưu trữ ở các file và những biến hoặc thành phần dữ liệu tương tự. Nhìn chung, những thành phần dữ liệu này được coi là cơ sở thông tin quản lý của thiết bị chịu sự quản lý. Xét riêng, mỗi thành phần dữ liệu biến đổi được coi là một đối tượng bị quản lý và bao gồm tên, một hoặc nhiều thuộc tính, và một tập các hoạt động (operation) thực hiện trên đối tượng đó. Vì vậy MIB định nghĩa loại thông tin có thể khôi phục từ một thiết bị chịu sự quản lý và những bố trí (settings) thiết bị mà có thể điều khiển từ hệ thống quản lí [5].

1.5.2.5 Các lệnh cơ bản trong SNMP

SNMP sử dụng các dịch vụ chuyển tải dữ liệu được cung cấp bởi các giao thức UDP/IP. Một ứng dụng của Manager phải nhận dạng được Agent cần thông tin với nó. Một ứng dụng của Agent được nhận dạng bởi địa chỉ IP của nó và một cổng UDP. Một ứng dụng Manager đóng gói yêu cầu SNMP trong một UDP/IP, UDP/IP chứa mã nhận dạng cổng nguồn, địa chỉ IP đích và mã nhận dạng cổng UDP của nó. Khung UDP sẽ được gửi đi thông qua thực thể IP tới hệ thống được quản lý, tới đó khung UDP sẽ được phân phối bởi thực thể UDP tới Agent. Tuong tự các bản tin TRAP phải được nhận dạng bởi các Manager. Các bản tin sử dụng địa chỉ IP và mã nhận dạng cổng UDP của Manager SNMP.

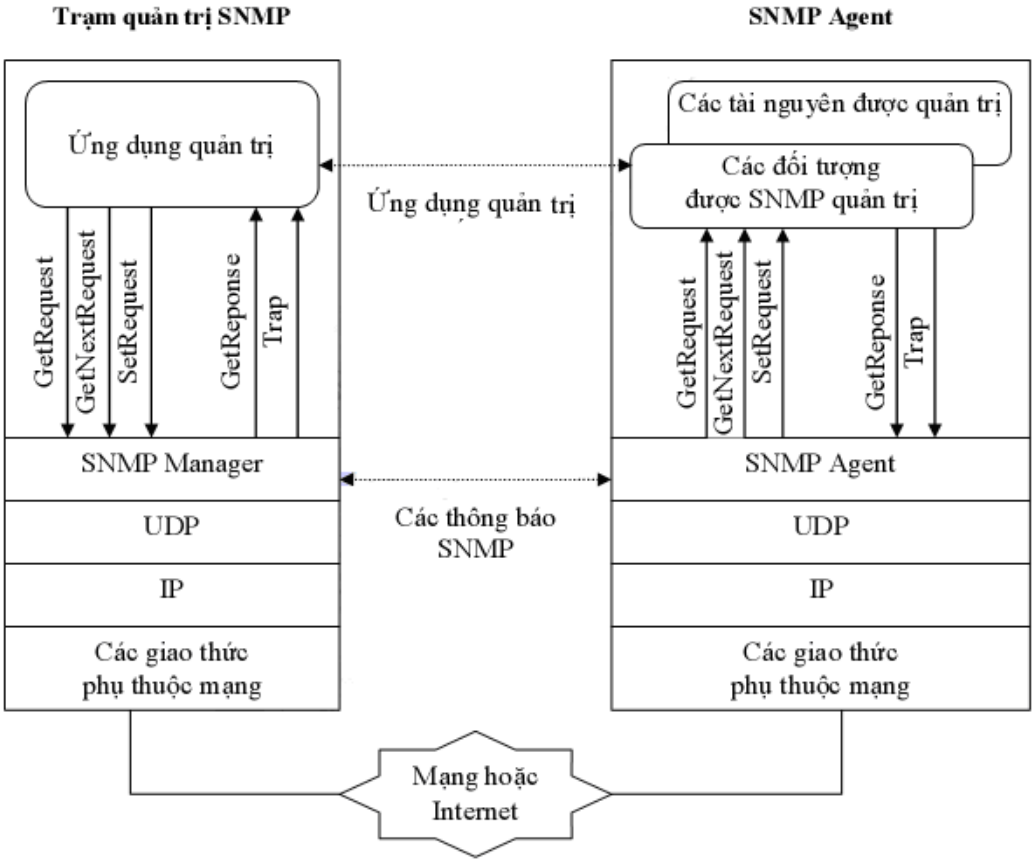
SNMP sử dụng 3 lệnh cơ bản là Read, Write, Trap số lệnh tùy biến để quản lý thiết bị.

Lệnh Read: Được SNMP dùng để dọc thông tin từ thiết bị. Các thông tin này được cung cấp qua các biến SNMP luu trữ trên thiết bị và được cập nhật bởi thiết bị.

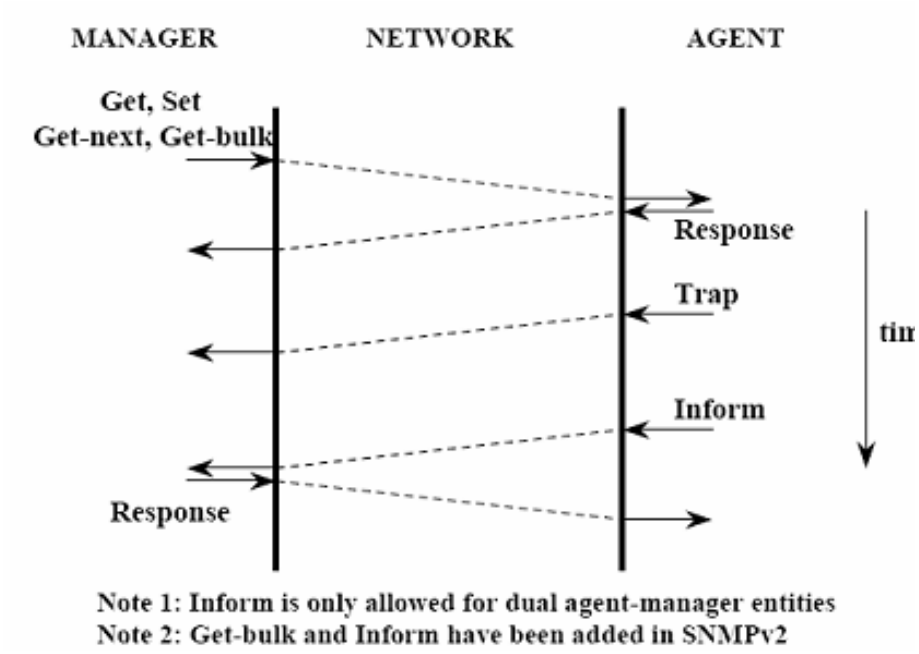
Lệnh Write: Được SNMP dùng để ghi các thông tin điều khiển lên thiết bị bằng cách thay đổi giá trị các biến SNMP.

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.

SNMP điều khiển, theo dõi thiết bị bằng cách thay đổi hoặc thu thập thông tin qua các biến giá trị lưu trên thiết bị. Các Agent cài đặt trên thiết bị tương tác với những chip điều khiển hỗ trợ SNMP để lấy nội dung hoặc viết lại nội dung.



Hình 1-1: Mô hình giao thức hoạt động SNMP



Hình 1-2: Hoạt động của giao thức SNMP

1.5.3 Quản lí liên lạc giữa management với các agent

Nhìn trên phương diện truyền thông, nhà quản lí (manager) và các tác nhân (agent) cũng là những người sử dụng, sử dụng một giao thức ứng dụng. Giao thức quản lý yên cầu cơ chế vận tải để hỗ trợ tương tác giữa các tác nhân và nhà quản lý.

Management trước hết phải xác định được các agent mà nó muốn liên lạc. Có thể xác định được ứng dụng tác nhân bằng địa chỉ IP của nó và cổng UDP được gán cho nó. Cổng UDP 161 được dành riêng cho các agent SNMP. Management gói lệnh SNMP vào một phong bì UDP/IP. Phong bì này chứa cổng nguồn, địa chỉ IP đích và cổng 161. Một thực thể UDP tại chỗ sẽ chuyển nó tới các agent. Tương tự như vậy, lệnh TRAP cũng cần xác định những management mà nó cần liên hệ. Chúng ta sử dụng địa chỉ IP cũng như cổng UDP dành cho management SNMP, đó là cổng 162.

1.5.4 Cơ chế vận chuyển thông tin giữa management và agent

Việc lựa chọn cơ chế vận chuyển có tính trực giao với giao thức truyền thông đó. SNMP chỉ đòi hỏi cơ chế truyền tải không tin cậy dữ liệu đồ (datagram) để truyền đưa các PDU (đơn vị dữ liệu giao thức) giữa

management và các agent. Điều này cho phép sự ánh xạ của SNMP tới nhiều nhóm giao thức. Mô hình vận chuyển datagram giảm được độ phức tạp của ánh xạ tầng vận chuyển. Tuy nhiên, vẫn phải nhận thức thấy sự tham gia của một số lựa chọn tầng vận chuyển. Các tầng vận chuyển khác nhau có thể sử dụng nhiều kỹ thuật đánh địa chỉ khác nhau. Các tầng vận chuyển khác nhau có thể đưa ra những hạn chế quy mô của PDU. Ánh xạ tầng vận chuyển có trách nhiệm phải xử lý các vấn đề đánh địa chỉ, hạn chế quy mô PDU và một số tham số tầng vận chuyển khác.

Trong phiên bản thứ hai của SNMP, người ta sử dụng kinh nghiệm để làm sắc nét và đơn giản hóa quá trình ánh xạ tới các chuẩn vận chuyển khác nhau. Giao thức quản lý được tách khỏi môi trường vận chuyển một cách trực giao, điều này cũng được khuyến khích sử dụng cho bất cứ nhóm giao thức nào.

1.5.5 Bảo vệ truyền thông liên lạc giữa management và các agent

Trong điều kiện mạng thiếu ổn định và thiếu độ tin cậy thì sẽ liên lạc quản lý càng trở nên quan trọng. Làm thế nào để các management liên lạc với các agent một cách tin cậy? Việc SNMP sử dụng cơ chế UDP để liên lạc đã có nghĩa là thiếu đi độ tin cậy. SNMP hoàn toàn để lại cho chương trình management chịu trách nhiệm và xử lý việc mất thông tin. Các lệnh GET, GET-NEXT, và SET đều được phúc đáp bằng một lệnh GET-RESPONSE. Hệ thống có thể dễ dàng phát hiện ra việc bị mất một lệnh khi không nhận được lệnh trả lại. Nó có thể lặp lại yêu cầu đó một lần nữa hoặc có những hành động khác. Tuy nhiên, các bản tin TRAP do agent tạo ra và không được phúc đáp khẳng định. Khi lệnh TRAP bị thất lạc, các chương trình agent sẽ không biết về điều đó (tất nhiên là management cũng không hay biết về điều này). Thông thường các bản tin TRAP mang những thông tin hết sức quan trọng cho management, do vậy management cần chú ý và cần bảo đảm việc chuyển phát chúng một cách tin cậy.

Một câu hỏi đặt ra là làm thế nào để chuyển phát các bản tin TRAP tránh mất mát, thất lạc? Ta có thể thiết kế cho các agent lặp lại bản tin TRAP. Biến số MIB có thể đọc số lần lặp lại theo yêu cầu. Lệnh SET của management có thể đặt cấu hình cho biến số này. Có một cách khác là agent có thể lặp lại lệnh TRAP cho đến khi management đặt biến số MIB để chấm dứt sự cố. Hãy ghi nhớ rằng, cả hai phương pháp trên đều chỉ cho ta những giải pháp từng phần. Trong trường hợp thứ nhất, số lần lặp lại có thể không đủ để đảm bảo liên lạc một cách tin cậy. Trong trường hợp thứ hai, một sự cố mạng có thể dẫn đến việc hàng loạt bản tin TRAP bị mất tùy thuộc vào tốc độ mà các agent tạo ra chúng. Điều này làm cho sự cố mạng trở nên trầm trọng hơn. Trong cả hai trường hợp, nếu ta cần chuyển phát những bản tin TRAP tới nhiều management, thì có thể xảy ra tình trạng không nhất quán giữa các management hoặc xảy ra hiện tượng thất lạc thông tin rất phức tạp. Nếu các agent phải chịu trách nhiệm về thiết kế cho việc phục hồi những bản tin TRAP thì càng làm tăng thêm độ phức tạp trong việc quản lý các agent trong môi trường đa nhà chế tạo. Người ta cũng đã theo đuổi cải tiến cơ chế xử lý bản tin sự cố cho phiên bản thứ hai của SNMP. Thứ nhất là đơn nguyên TRAP được bỏ đi và thay thế nó bằng một lệnh GET/RESPONSE không yêu cầu. Lệnh này do agent tạo ra và chuyển đến cho "management bẫy" tại cổng UDP-162. Điều này phản ánh một quan điểm là nhà quản lý sự cố có thể thống nhất các bản tin sự cố rồi trả lại cho các yêu cầu ảo. Bằng cách bỏ đi một đơn thể, giao thức được đơn giản hóa. Người ta cũng bổ sung thêm một cơ sở thông tin quản lý đặc biệt TRAP MIB để thống nhất việc xử lý sự cố, các management nhận bản tin về các sự cố này và việc lặp lại để cải thiện độ tin cậy trong chuyển phát thông tin.

1.5.6 Các phương thức của SNMP

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

Bản tin/phương thức	Mô tả tác dụng
GetRequest	Manager gửi GetRequest cho agent để yêu cầu agent cung cấp thông tin nào đó dựa vào ObjectID (trong GetRequest có chứa OID)
GetNextRequest	Manager gửi GetNextRequest có chứa một ObjectID cho agent để yêu cầu cung cấp thông tin nằm kế tiếp ObjectID đó trong MIB.
SetRequest	Manager gửi SetRequest cho agent để đặt giá trị cho đối tượng của agent dựa vào ObjectID.
GetResponse	Agent gửi GetResponse cho Manager để trả lời khi nhận được GetRequest/GetNextRequest
Trap	Agent tự động gửi Trap cho Manager khi có một sự kiện xảy ra đối với một object nào đó trong agent.

Hình 1-3: Bảng các phương thức cơ bản của SNMP

Mỗi bản tin đều có chứa OID để cho biết object mang trong nó là gì. OID trong GetRequest cho biết nó muốn lấy thông tin của object nào. OID trong GetResponse cho biết nó mang giá trị của object nào. OID trong SetRequest chỉ ra nó muốn thiết lập giá trị cho object nào. OID trong Trap chỉ ra nó thông báo sự kiện xảy ra đối với object nào.

1.5.6.1 GetRequest

Bản tin GetRequest được manager gửi đến agent để lấy một thông tin nào đó. Trong GetRequest có chứa OID của object muốn lấy. VD: Muốn lấy thông tin tên của Device1 thì manager gửi bản tin GetRequest OID= 1.3.6.1.2.1.1.5 đến Device1, tiến trình SNMP agent trên Device1 sẽ nhận được bản tin và tạo bản tin trả lời. Trong một bản tin GetRequest có thể chứa nhiều OID, nghĩa là dùng một GetRequest có thể lấy về cùng lúc nhiều thông tin.

1.5.6.2 GetNextRequest

Bản tin GetNextRequest cũng dùng để lấy thông tin và cũng có chứa OID, tuy nhiên nó dùng để lấy thông tin của object nằm kế tiếp object được chỉ ra trong bản tin.

Tại sao phải có phương thức GetNextRequest? Như bạn đã biết khi đọc qua những phần trên: một MIB bao gồm nhiều OID được sắp xếp thứ tự nhưng không liên tục, nếu biết một OID thì không xác định được OID kế tiếp.

Do đó ta cần GetNextRequest để lấy về giá trị của OID kế tiếp. Nếu thực hiện GetNextRequest liên tục thì ta sẽ lấy được toàn bộ thông tin của agent.

1.5.6.3 SetRequest

Bản tin SetRequest được manager gửi cho agent để thiết lập giá trị cho một object nào đó.

Ví dụ:

- Có thể đặt lại tên của một máy tính hay Router bằng phần mềm SNMP manager, bằng cách gửi bản tin SetRequest có OID là 1.3.6.1.2.1.1.5.0 (sysName.0) và có giá trị là tên mới cần đặt.
- Có thể shutdown một port trên Switch bằng phần mềm SNMP manager, bằng cách gửi bản tin có OID là 1.3.6.1.2.1.2.2.1.7 (ifAdminStatus) và có giá trị là 2 7. Chỉ những object có quyền READ_WRITE mới có thể thay đổi được giá trị.

1.5.6.4 GetResponse

Mỗi khi SNMP agent nhận được các bản tin GetRequest, GetNextRequest hay SetRequest thì nó sẽ gửi lại bản tin GetResponse để trả lời. Trong bản tin GetResponse có chứa OID của object được request và giá trị của object đó.

1.5.6.5 Trap

Bản tin Trap được agent tự động gửi cho manager mỗi khi có sự kiện xảy ra bên trong agent, các sự kiện này không phải là các hoạt động thường xuyên của agent mà là các sự kiện mang tính biến cố. Ví dụ: Khi có một port down, khi có một người dùng login không thành công, hoặc khi thiết bị khởi động lại, agent sẽ gửi trap cho manager.

Tuy nhiên không phải mọi biến cố đều được agent gửi trap, cũng không phải mọi agent đều gửi trap khi xảy ra cùng một biến cố. Việc agent gửi hay không gửi trap cho biến cố nào là do hãng sản xuất device/agent quy định.

Phương thức trap là độc lập với các phương thức request/response. SNMP request/response dùng để quản lý còn SNMP trap dùng để cảnh báo. Nguồn gửi trap gọi là Trap Sender và nơi nhận trap gọi là Trap Receiver. Một trap sender có thể được cấu hình để gửi trap đến nhiều trap receiver cùng lúc. Có 2 loại trap : trap phổ biến (generic trap) và trap đặc thù (specific trap). Generic trap được quy định trong các chuẩn SNMP, còn specific trap do người dùng tự định nghĩa (người dùng ở đây là hãng sản xuất SNMP device). Loại trap là một số nguyên chứa trong bản tin trap, dựa vào đó mà phía nhận trap biết bản tin trap có nghĩa gì [7].

Theo SNMPv1, generic trap có 7 loại sau: coldStart(0), warmStart(1), linkDown(2), linkUp(3), authenticationFailure(4), egpNeighborloss(5), enterpriseSpecific(6).

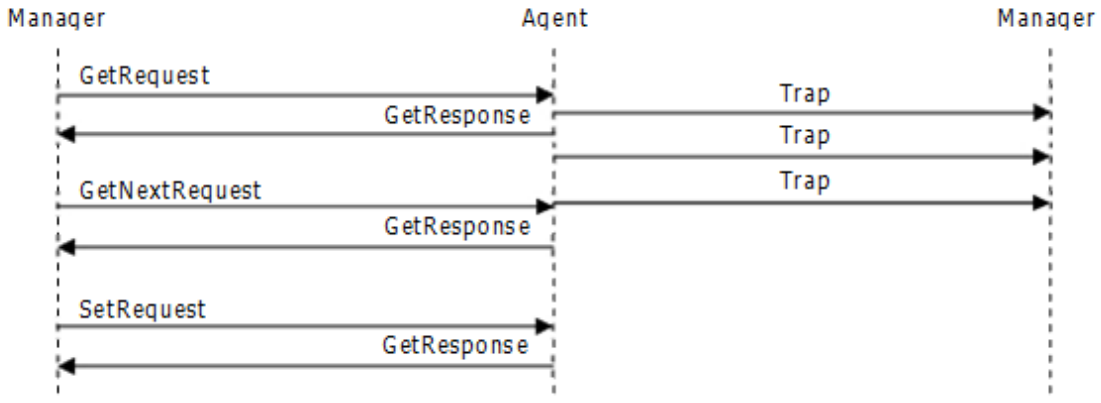
Giá trị trong ngoặc là mã số của các loại trap. Ý nghĩa của các bản tin generic-trap như sau:

- ColdStart: thông báo rằng thiết bị gửi bản tin này đang khởi động lại (reinitialize) và cấu hình của nó có thể bị thay đổi sau khi khởi động.
- WarmStart: thông báo rằng thiết bị gửi bản tin này đang khởi động lại và giữ nguyên cấu hình cũ.
- LinkDown: thông báo rằng thiết bị gửi bản tin này phát hiện được một trong những kết nối truyền thông (communication link) của nó gặp lỗi. Trong bản tin trap có tham số chỉ ra ifIndex của kết nối bị lỗi.
- LinkUp: thông báo rằng thiết bị gửi bản tin này phát hiện được một trong những kết nối truyền thông của nó đã khôi phục trở lại. Trong bản tin trap có tham số chỉ ra ifindex của kết nối được khôi phục.
- AuthenticationFailure: thông báo rằng thiết bị gửi bản tin này đã nhận được một bản tin không được chứng thực thành công (bản tin bị chứng thực không thành công có thể thuộc nhiều giao thức khác nhau như

telnet, ssh, snmp, ftp, …). Thông thường trap loại này xảy ra là do user đăng nhập không thành công vào thiết bị.

- EgpNeighborloss: thông báo rằng một trong số những "EGP neighbor" 8 của thiết bị gửi trap đã bị coi là down và quan hệ đối tác (peer relationship) giữa 2 bên không còn được duy trì.
- EnterpriseSpecific: thông báo rằng bản tin trap này không thuộc các kiểu generic như trên mà nó là một loại bản tin do người dùng tự định nghĩa.

Người dùng có thể tự định nghĩa thêm các loại trap để làm phong phú thêm khả năng cảnh báo của thiết bị như: boardFailed, configChanged, powerLoss, cpuTooHigh, v.v…. Người dùng tự quy định ý nghĩa và giá trị của các specific trap này, và dĩ nhiên chỉ những trap receiver và trap sender hỗ trợ cùng một MIB mới có thể hiểu ý nghĩa của specific trap. Do đó nếu bạn dùng một phần mềm trap receiver bất kỳ để nhận trap của các trap sender bất kỳ, bạn có thể đọc và hiểu các generic trap khi chúng xảy ra, nhưng bạn sẽ không hiểu ý nghĩa các specific trap khi chúng hiện lên màn hình vì bản tin trap chỉ chứa những con số.



Hình 1-4: Minh họa các phương thức SNMPv1

Đối với các phương thức Get/Set/Response thì SNMP Agent lắng nghe ở port UDP 161, còn phương thức trap thì SNMP Trap Receiver lắng nghe ở port UDP 162.

1.5.7 Các cơ chế bảo mật cho SNMP

Một SNMP management station có thể quản lý/giám sát nhiều SNMP element, thông qua hoạt động gửi request và nhận trap. Tuy nhiên một SNMP element có thể được cấu hình để chỉ cho phép các SNMP management station nào đó được phép quản lý/giám sát mình.

Các cơ chế bảo mật đơn giản này gồm có: community string, view và SNMP access control list.

1.5.7.1 Community string

Community string là một chuỗi ký tự được cài đặt giống nhau trên cả SNMP manager và SNMP agent, đóng vai trò như "mật khẩu" giữa 2 bên khi trao đổi dữ liệu. Community string có 3 loại: Read-community, Write-Community và Trap-Community.

Khi manager gửi GetRequest, GetNextRequest đến agent thì trong bản tin gửi đi có chứa Read-Community. Khi agent nhận được bản tin request thì nó sẽ so sánh Read-community do manager gửi và Read-community mà nó được cài đặt. Nếu 2 chuỗi này giống nhau, agent sẽ trả lời, nếu 2 chuỗi này khác nhau, agent sẽ không trả lời.

Write-Community được dùng trong bản tin SetRequest. Agent chỉ chấp nhận thay đổi dữ liệu khi write-community 2 bên giống nhau.

Trap-community nằm trong bản tin trap của trap sender gửi cho trap receiver. Trap receiver chỉ nhận và lưu trữ bản tin trap chỉ khi trap-community 2 bên giống nhau, tuy nhiên cũng có nhiều trap receiver được cấu hình nhận tất cả bản tin trap mà không quan tâm đến trap-community.

Community string có 3 loại như trên nhưng cùng một loại có thể có nhiều string khác nhau. Nghĩa là một agent có thể khai báo nhiều read-community, nhiều write-community.

Trên hầu hết hệ thống, read-community mặc định là “public”, write-community mặc định là “private” và trap-community mặc định là “public”.

Community string chỉ là chuỗi ký tự dạng cleartext, do đó hoàn toàn có thể bị nghe lén khi truyền trên mạng. Hơn nữa, các community mặc định thường là “public” và “private” nên nếu người quản trị không thay đổi thì chúng có thể dễ dàng bị dò ra. Khi community string trong mạng bị lộ, một người dùng bình thường tại một máy tính nào đó trong mạng có thể quản lý/giám sát toàn bộ các device có cùng community mà không được sự cho phép của người quản trị.

1.5.7.2 View

Khi manager có read-community thì nó có thể đọc toàn bộ OID của agent. Tuy nhiên agent có thể quy định chỉ cho phép đọc một số OID có liên quan nhau, tức là chỉ đọc được một phần của MIB. Tập con của MIB này gọi là view, trên agent có thể định nghĩa nhiều view. Ví dụ: agent có thể định nghĩa view interfaceView bao gồm các OID liên quan đến interface, storageView bao gồm các OID liên quan đến lưu trữ, hay AllView bao gồm tất cả các OID.

Một view phải gắn liền với một community string. Tùy vào community string nhận được là gì mà agent xử lý trên view tương ứng. Ví dụ: agent định nghĩa read-community “inf” trên view interfaceView, và “sto” trên storageView; khi manager gửi request lấy OID ifNumber với community là “inf” thì sẽ được đáp ứng do ifNumber nằm trong interfaceView; nếu manager request OID hrStorageSize với community “inf” thì agent sẽ không trả lời do hrStorageSize không nằm trong interfaceView; nhưng nếu manager request hrStorageSize với community “sto” thì sẽ được trả lời do hrStorageSize nằm trong storageView.

Việc định nghĩa các view như thế nào tùy thuộc vào từng SNMP agent khác nhau. Có nhiều hệ thống không hỗ trợ tính năng view [7].

1.5.7.3 SNMP access control list

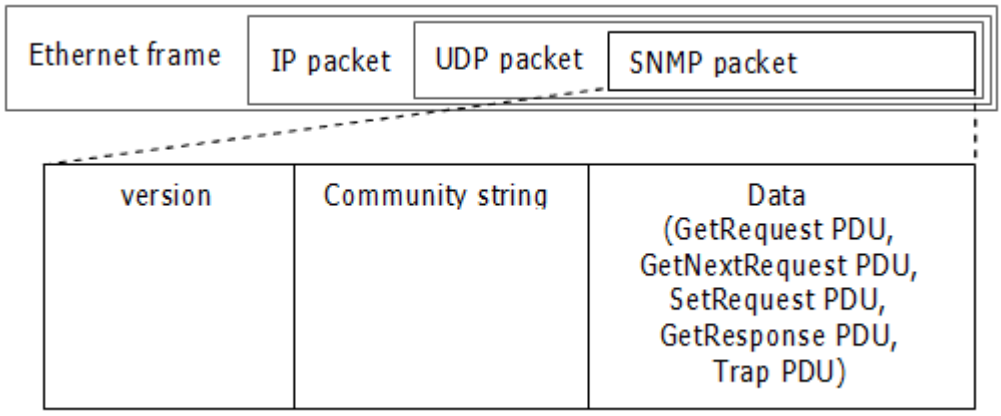
Khi manager gửi không đúng community hoặc khi OID cần lấy lại không nằm trong view cho phép thì agent sẽ không trả lời. Tuy nhiên khi community bị lộ thì một manager nào đó vẫn request được thông tin.

Để ngăn chặn hoàn toàn các SNMP manager không được phép, người quản trị có thể dùng đến SNMP access control list (ACL). SNMP ACL là một danh sách các địa chỉ IP được phép quản lý/giám sát agent, nó chỉ áp dụng riêng cho giao thức SNMP và được cài trên agent. Nếu một manager có IP không được phép trong ACL gửi request thì agent sẽ không xử lý, dù request có community string là đúng.

Đa số các thiết bị tương thích SNMP đều cho phép thiết lập SNMP ACL.

1.5.8 Cấu trúc bản tin SNMP

SNMP chạy trên UDP. Cấu trúc của một bản tin SNMP bao gồm: version, community và data.



Hình 1-5: Cấu trúc bản tin SNMP Version: v1= 0, v2c= 1, v2u= 2, v3= 3.

Phần Data trong bản tin SNMP gọi là PDU (Protocol Data Unit). SNMPv1 có 5 phương thức hoạt động tương ứng 5 loại PDU. Tuy nhiên chỉ có 2 loại định dạng bản tin là PDU và Trap-PDU, trong đó các bản tin Get, GetNext, Set, GetResponse có cùng định dạng là PDU, còn bản tin Trap có định dạng là Trap-PDU.

CHƯƠNG 2: PHẦN MỀM GIÁM SÁT HỆ THỐNG MẠNG NAGIOS

2.1 Giới thiệu 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.

Đầu tiên ra mắt vào năm 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 sản phẩm dịch vụ.

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.

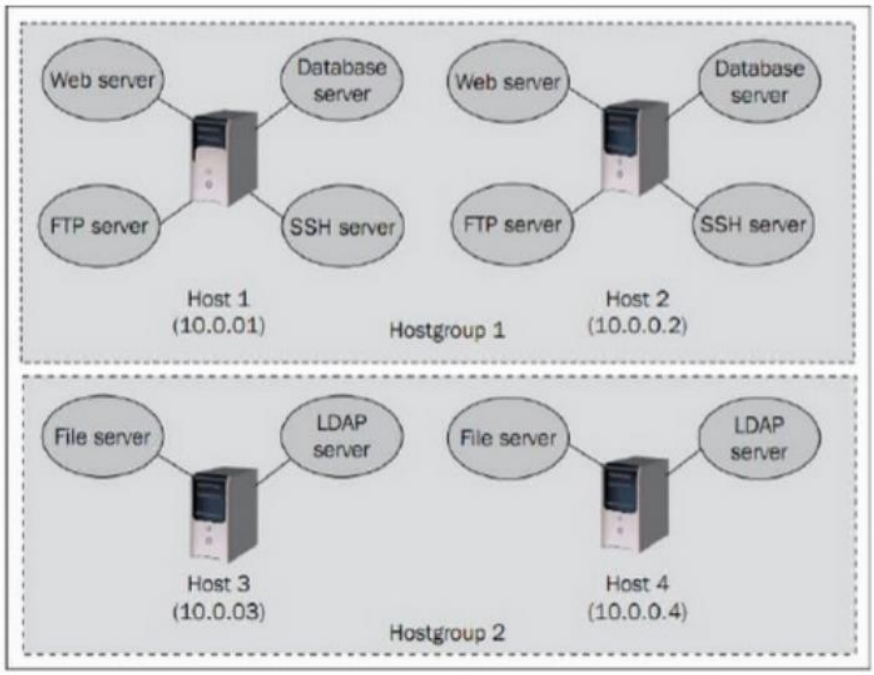
Nagios có hai ưu điểm lớn khi nói đến quá trình giám sát, thay vì theo dõi các giái trị, nó chỉ sử dụng bốn mức độ để mô tả tình trạng: OK, WARNING, CRITICAL và UNKNOW. Các mô tả tình trạng của các đối tượng giám sát cho phép người quản trị giải quyết hay bỏ các vấn đề trên hệ thống mà không tốn nhiều 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 2-1: 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 ra muốn thực thi một kiểm tra đặc biệt ta có thể tạo một plugins cho riêng mình [3].

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, cở sở dữ liệu: mysql, portgreSQL, 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): tình trạng sử dụng CPU, người dùng đang log on, tình trạng sử dụng ổ đĩa cứng, tình trạng sử dụng bộ nhớ trong và swap, số tiến trình đang chạy, các tệp log hệ thống.

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 sảy 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 về tình trạng hoạt động của mạng [4].

2.3 Đặc điểm của Nagios

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 thi 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 [4].

2.4 Kiến trúc và tổ chức hoạt động

2.4.1 Kiến trúc của Nagios

Hệ thống Nagios gồm hai phần chính:

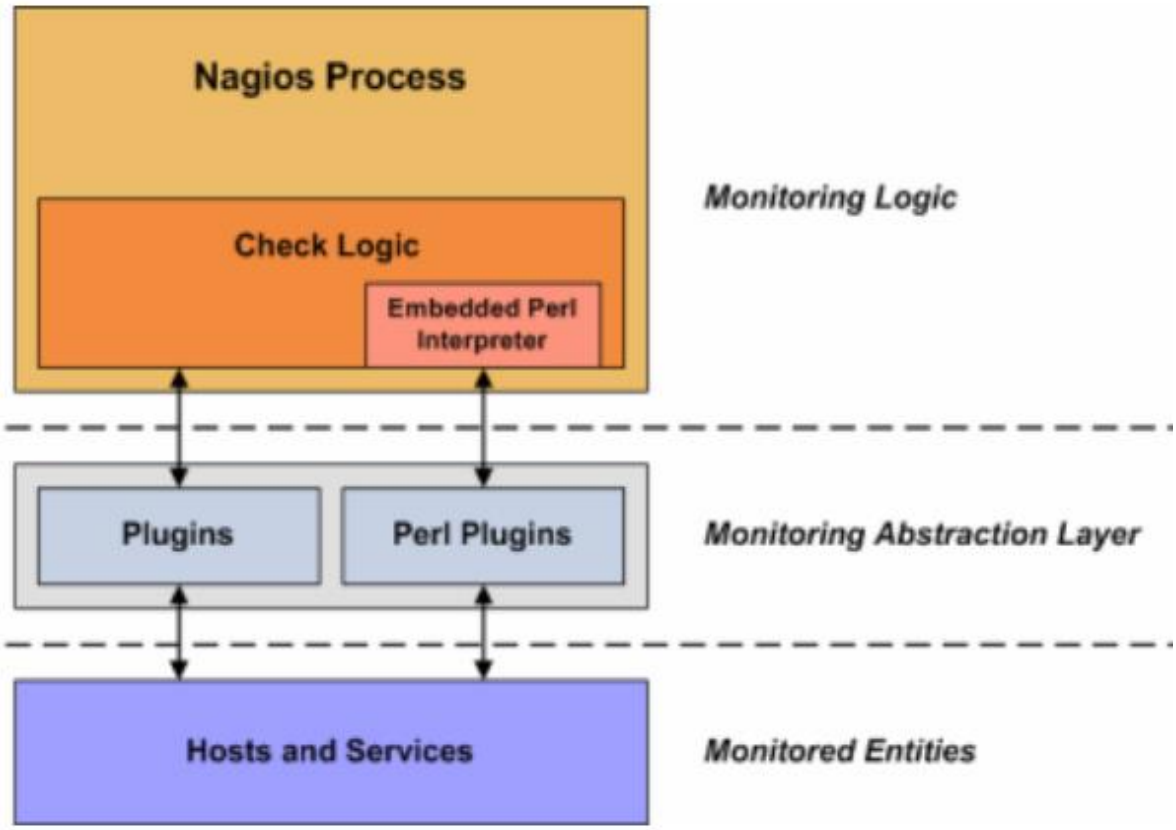
1. Lõi Nagios

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.

2. Plugin

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 [4].



Hình 2-2: Sơ đồ tổ chức của Nagios

2.4.2 Cách thức tổ chức hoạt động

Nagios có 5 cách thực thi các hành động kiểm tra:

2.4.2.1 Kiểm tra dịch vụ trực tiếp.

Đối với các dịch vụ mạng có giao thức giao tiếp qua mạng như smtp, http, ftp... Nagios có thể tiến hành kiểm tra trực tiếp một dịch vụ xem nó hoạt động hay không bằng cách gửi truy vấn kết nối dịch vụ đến server dịch vụ và đợi kết quả trả về. Các plugins phục vụ kiểm tra này được đặt ngay trên server Nagios.

2.4.2.2 Chạy các plugin trên máy ở xa bằng secure shell

Nagios server không có cách nào có thể truy cập trực tiếp client để theo dõi những thông tin như tình trạng sử dụng ổ đĩa, swap, tiến trình ... Để làm được việc này thi trên máy được giám sát phải cài plugin cục bộ. Nagios sẽ điều khiển các plugin cục bộ trên client qua secure shell ssh bằng plguin *check_by_ssh*. Phương pháp này yêu cầu một tài khoản truy cập host được giám sát nhưng nó có thể thực thi được tất cả các plugin được cài trên host đó.

2.4.2.3 Bộ thực thi plugin từ xa (NPRE- Nagios Remote Plugin Executor)

NRPE là một addon đi kèm với Nagios. Nó trợ giúp việc thực thi các plugin được cài đặt trên máy/thiết bị được giám sát. NRPE được cài trên các host được giám sát. Khi nhận được truy vấn từ Nagios server thì nó gọi các plugin cục bộ phù hợp trên host này, thực hiện kiểm tra và trả về kết quả cho Nagios server. Phương pháp này không đòi hỏi tài khoản truy cập host được giám sát như sử dụng ssh. Tuy nhiên cũng như ssh các plugin phục vụ giám sát phải được cài đặt trên host được giám sát. NRPE có thể thực thi được tất cả các loại plugin giám sát. Nagios có thể điều khiển máy cài NRPE kiểm tra các thông số phần cứng, các tài nguyên, tình trạng hoạt động của máy đó hoặc sử dụng NRPE để thực thi các plugin yêu cầu truy vấn dịch vụ mạng đến một máy thứ 3 để kiểm tra hoạt động của các dịch vụ mạng như http, ftp, mail…

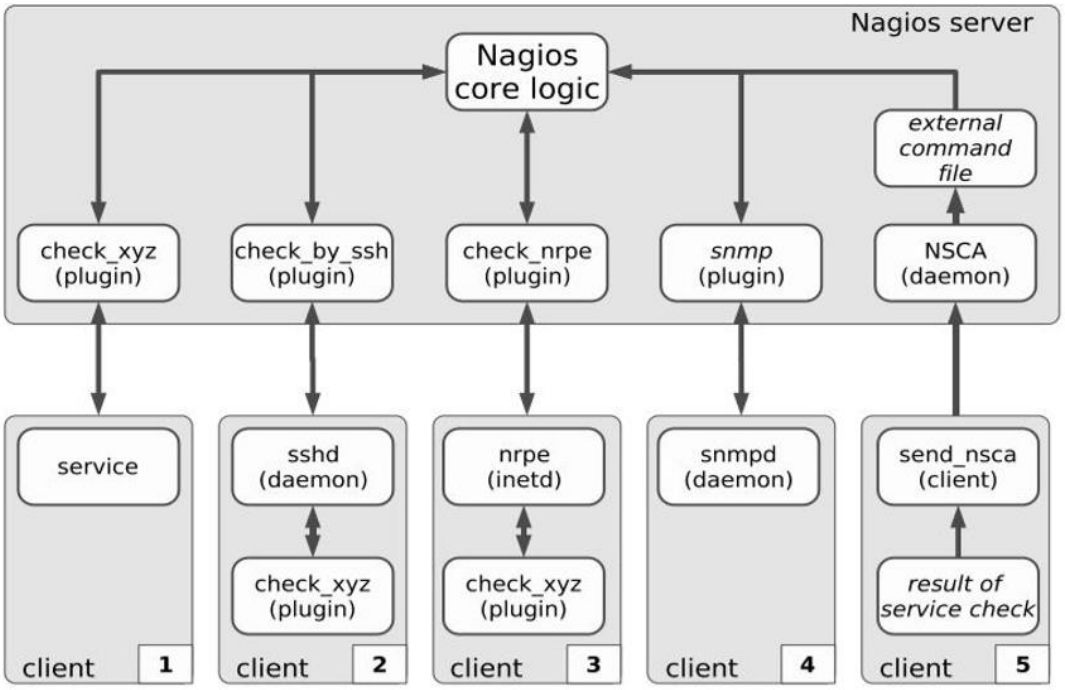
2.4.2.4 Giám sát qua SNMP

Cốt lõi của giao thức SNMP (SimpleNetwork Management Protocol) là tập hợp đơn giản các hoạt động giúp nhà quản trị mạng có thể quản lý, thay đổi trạng thái thiết bị. Hiện nay rất nhiều thiết bị mạng hỗ trợ giao thức

SNMP như Switch, Router, máy in, firewall ... Nagios cũng có khả năng sử dụng giao thức SNMP để theo dõi trạng thái của các client, các thiết bị mạng có hỗ trợ SNMP. Qua SNMP, Nagios có được thông tin về tình trạng hiện thời của thiết bị. Ví dụ như với SNMP, Nagios có thể biết được các cổng của Switch, Router có mở hay không, thời gian Uptime (chạy liên tục) là bao nhiêu…

2.4.2.5 NSCA (Nagios Service Check Acceptor)

Nagios được coi là một phần mềm rất mạnh vì nó dễ dàng được mở rộng và kết hợp với các phần mềm khác. Nó có thể tổng hợp thông tin từ các phần mềm kiểm tra của hãng thứ ba hoặc các tiến trình Nagios khác về trạng thái của host/dịch vụ. Như thế Nagios không cần phải lập lịch và chạy các hành động kiểm tra host/dịch vụ mà các ứng dụng khác sẽ thực hiện điều này và báo cáo thông tin về cho nó. Và các ứng dụng kiểm tra có thể tận dụng được khả năng rất mạnh của Nagios là thông báo và tổng hợp báo cáo. Nagios sử dụng công cụ NSCA để gửi các kết quả kiểm tra từ ứng dụng của bạn về server Nagios. Công cụ này giúp cho thông tin gửi trên mạng được an toàn hơn vì nó được mã hóa và xác thực.



Hình 2-3: Các cách thức hiện kiểm tra

Hình trên cho ta cái nhìn tổng quan về các cách thức kiểm tra dịch vụ với nagios. Có 5 client được giám sát bằng 5 cách thức khác nhau:

Client 1: Nagios sử dụng plugin 'check_xyz' được cài đặt ngay trên server Nagios để gửi truy vấn kiểm tra dịch vụ trên client (http, ftp, dns, smtp…)

Client 2, 3: Nagios sử dụng các plugin trung gian để chạy plugin 'check_xyz' giám sát được cài đặt trực tiếp trên client. (bởi vì có những dịch vụ không có hỗ trợ giao thức trao đổi qua mạng, ví dụ khi bạn muốn kiểm tra dung lượng ổ đĩa cứng còn trống trên client…)

Client 4: Kiểm tra dịch vụ qua giao thức snmp, nagios server sẽ sử dụng plugin check_snmp để kiểm tra các dịch vụ trên client có hỗ trợ giao thức SNMP. Rất nhiều thiết bị mạng như Router, Switch, máy in… có hỗ trợ giao thức SNMP.

Client 5: Đây là phương pháp kiểm tra bị động. Nagios không chủ động kiểm tra dịch vụ mà là client chủ động gửi kết quả kiểm tra dịch vụ về cho Nagios thông qua plugin NSCA. Phương pháp này được áp dụng nhiều trong giám sát phân tán. Với các mạng có quy mô lớn, người ta có thể dùng nhiều server Nagios để giám sát từng phần của mạng. Trong đó có một server Nagios trung tâm thực hiện tổng hợp kết quả từ các server Nagios con thông qua plugin NSCA.

2.5 Cấu hình nagios

2.5.1 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.

2.5.2 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(contactgroups), 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

2.6 Cách thức định nghĩa đối tượng trong các tệp cấu hình đối tượng

Các đối tượng (bao gồm host, dịch vụ, người liên hệ, lệnh, nhóm, chu kỳ thời gian) có thể đươc định nghĩa trong bất kì tệp nào có đuôi .cfg và khai báo đường dẫn trong tệp cấu hình chính qua tùy chọn cfg_file. Tệp template.cfg đã có sẵn những định nghĩa đối tượng chuẩn, các định nghĩa đối tượng mới có thể kế thừa khuôn mẫu của định nghĩa chuẩn và có thể thay đổi đi một số tùy chọn cho phù hợp với từng yêu cầu sử dụng [4].

2.6.1 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 với host khác.

Khi định nghĩa đối tượng host bạn có thể kế thừa mẫu định nghĩa host có trong tệp template.cfg. Mẫu định nghĩa này có trong phần phụ lục cuối tài liệu. Tuy nhiên với mỗi host được định nghĩa mới 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 //kế thừa định nghĩa mẫu có sẵn
host_name
fedora10
alias          f10
address        192.168.89.128 …  }
```

2.6.2 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 là POP, SMTP, HTTP… hay là 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 thừa 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}
```

2.6.3 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.

Khuôn dạng của một lệnh được định nghĩa:

define command {

command_name Tên lệnh

command_line Người dùng/script! Danh sách tham số}

2.6.4 Các định nghĩa khác

Ngoài ra còn các định nghĩa khác như nhóm host, nhóm dịch vụ, nhóm liên lạc, chu kỳ thời gian được giới thiệu trong phần phụ lục của tài liệu [4] ...

2.7 Cài đặt phần mềm nagios

2.7.1 Yêu cầu hệ thống

Server: CPU duo core, RAM >= 1GB, HDD >=50 GB 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

2.7.2 Các gói yêu cầu trước khi cài đặt Nagios

Đảm bảo các gói sau được cài đặt trước tiếp tục cài Nagios:

Apache, PHP, GCC compiler, GD development libraries

Sử dụng lệnh:

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

2.7.3 Tạo thông tin tài khoản

Tạo một tài khoản người dùng Nagios mới và đặt mật khẩu

/usr/sbin/useradd –m nagios

Passwd nagios

Tạo một nhóm mới có tên là nagcmd cho phép các lệnh ngoại trú được submit qua giao diện web. Thêm tài khoản người dùng nagios và người dùng apache vào nhóm này.

/usr/sbin/groupadd nagcmd

/usr/sbin/usermod -a -G nagcmd nagios

/usr/sbin/usermod -a -G nagcmd apache

2.7.4 Tải về Nagios và Plugin

Tạo thư mục để lưu trữ mã nguồn mở dowload

Mkdir /home/source

Cd /home/source

Có thể vào website **httpd://www.nagios.org/dowload/** để tải về phiên bản mới nhất của Nagios và Plugin. Hoặc thực hiện dowload phiên bản Nagios 4.0.8 và Nagios Plugin 2.0.3 bằng lệnh [2]:

Wgethttpd://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz

Wgethttpd://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-2.0.3.tar.gz

2.7.5 Biên dịch và cài đặt Nagios

Giải nén mã nguồn Nagios

Cd /home/source

tar xzf nagios-4.0.8.tar.gz

cd nagios-4.0.8

chạy script cấu hình, với tham số là tên của nhóm vừa tạo

./configure --with-command-group=nagcmd

Biên dịch mã nguồn Nagios:

make all

Cài đặt nhị phân, script khởi tạo, tệp cấu hình mẫu và đặt quyền trên thư mục lệnh ngoại trú (external command).

make install

make install-init

make install-config

make install-commandmode

2.7.6 Tùy chỉnh cấu hình

Tệp cấu hình mẫu được đặt trong thư mục */usr/local/nagios/etc*.

Mở tệp cấu hình /usr/local/etc/objects/contacts.cfg

Thay đổi địa chỉ email trong phần nagiosadmin thành địa chỉ email của người sẽ nhận cảnh báo các nguy cơ của mạng từ Nagios

```
#       You don't need to keep these definitions in a separate file from your
#       other object definitions.  This has been done just to make things
#       easier to understand.
#
###############################################################################



###############################################################################
###############################################################################
#
# CONTACTS
#
###############################################################################
###############################################################################

# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the 'generic-contact'
# template which is defined elsewhere.

define contact{
        contact_name                    nagiosadmin             ; Short name of user
        use                             generic-contact         ; Inherit default values from generic-contact template (defined above)
        alias                           Nagios Admin            ; Full name of user

        email                           quanganhhp23@gmail.com  ; <<***** CHANGE THIS TO YOUR EMAIL ADDRESS ******
        }
```

Hình 2-4: Thay đổi email trong nagiosadmin

2.7.7 Cấu hình giao diện web

Cài đặt tệp cấu hình mẫu của Nagios vào thư mục conf.d của apache

Make install-webconf

Tạo tài khoản nagiosadmin để đăng nhập vào Nagios qua giao diện web. Đặt mật khẩu:

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

Khởi động lại Apache

service httpd restart

2.7.8 Biên dịch và cài đặt các Nagios Plugin

Giải nén mã nguồn Nagios plugins.

Cd /home/source

tar xzf nagios-plugins-1.4.11.tar.gz

cd nagios-plugins-1.4.11

Cài đặt

./configure --with-nagios-user=nagios --with-nagios-group=nagios

make

make install

2.7.9 Khởi động Nagios

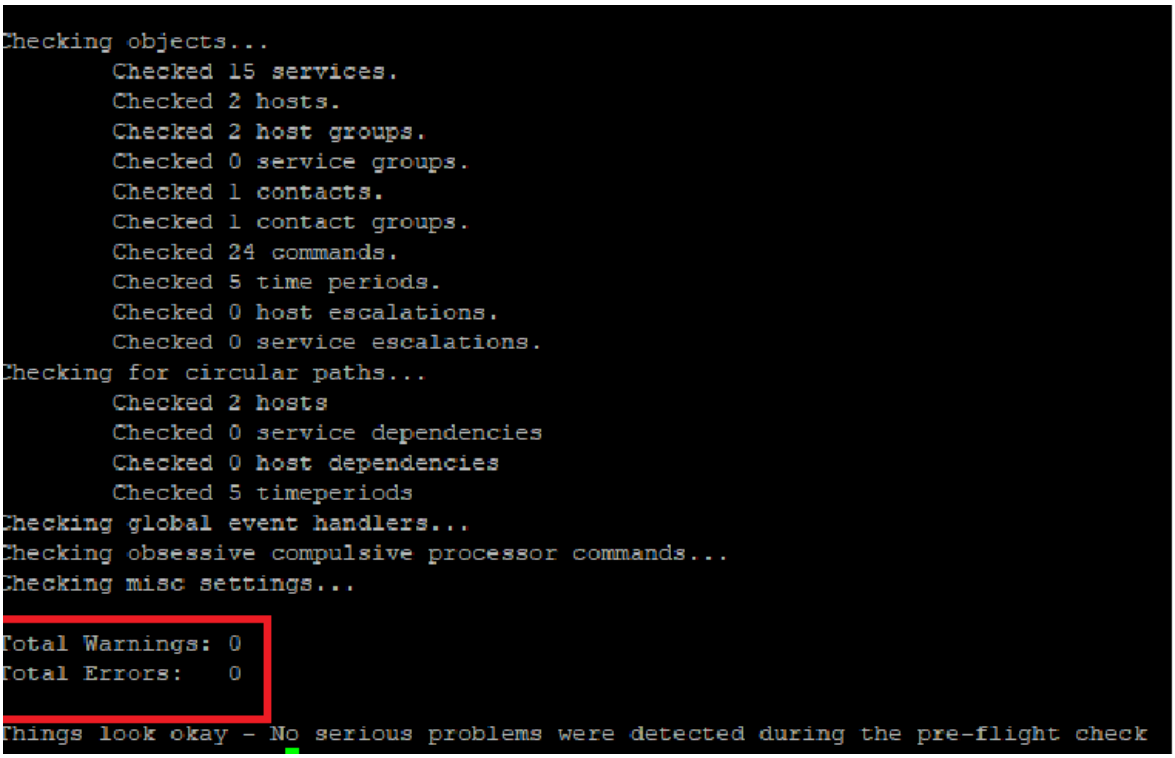
Thêm nagios vào danh sách các dịch vụ tự động khởi động với hệ thống.

chkconfig --add nagios

chkconfig nagios on

Kiểm tra file cấu hình Nagios

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg



Hình 2-5: Kiểm tra lỗi

Nếu không có lỗi xảy ra, khởi động nagios

service nagios start

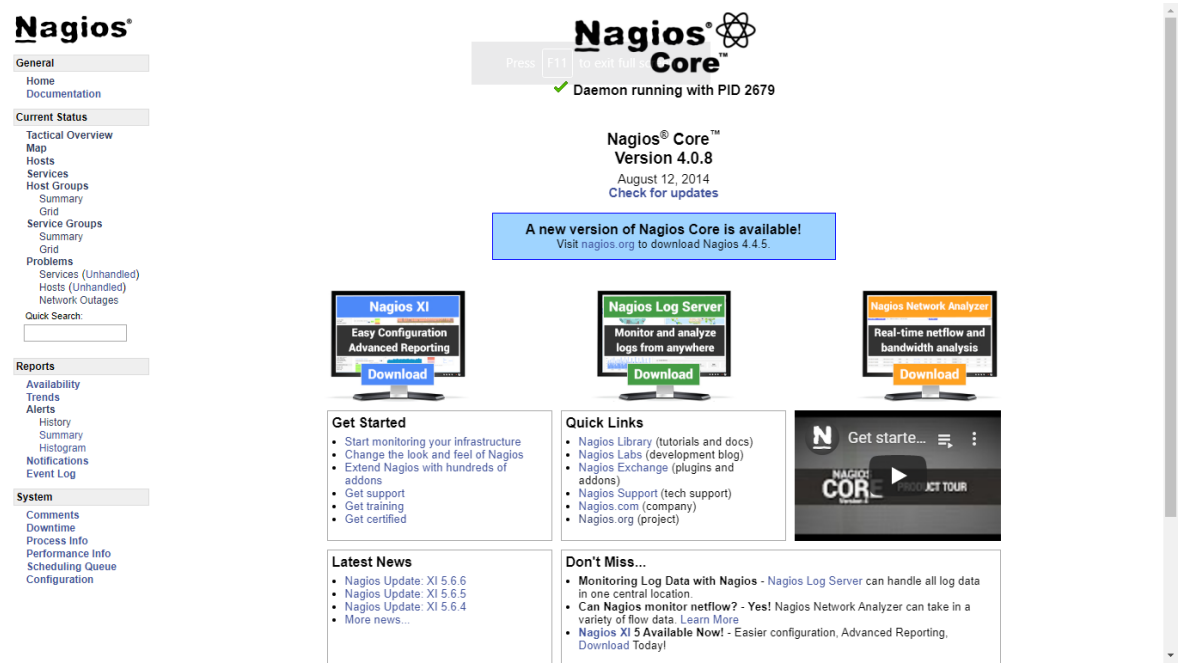
Đặt selinux ở kiểu permissive

setenforce 0

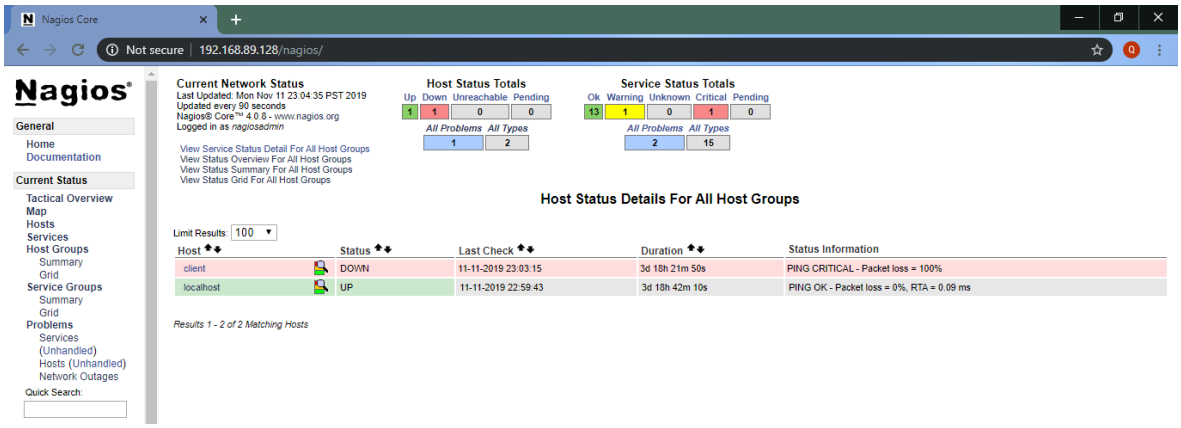
Tắt tưởng lửa

service iptables stop

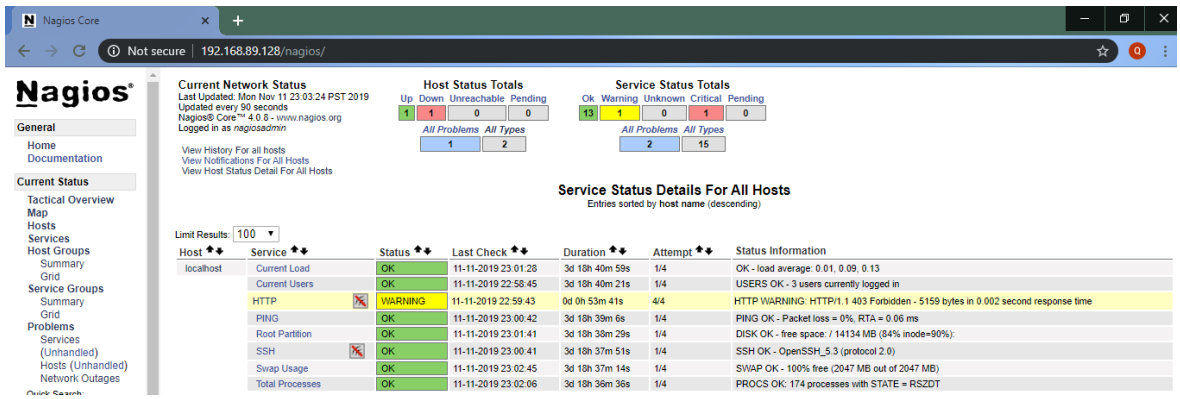
truy cập nagios: http://ip_hoặc_tên_miền/nagios



Hình 2-6: Khởi động nagios



Hình 2-7: Kiểm tra host monitor



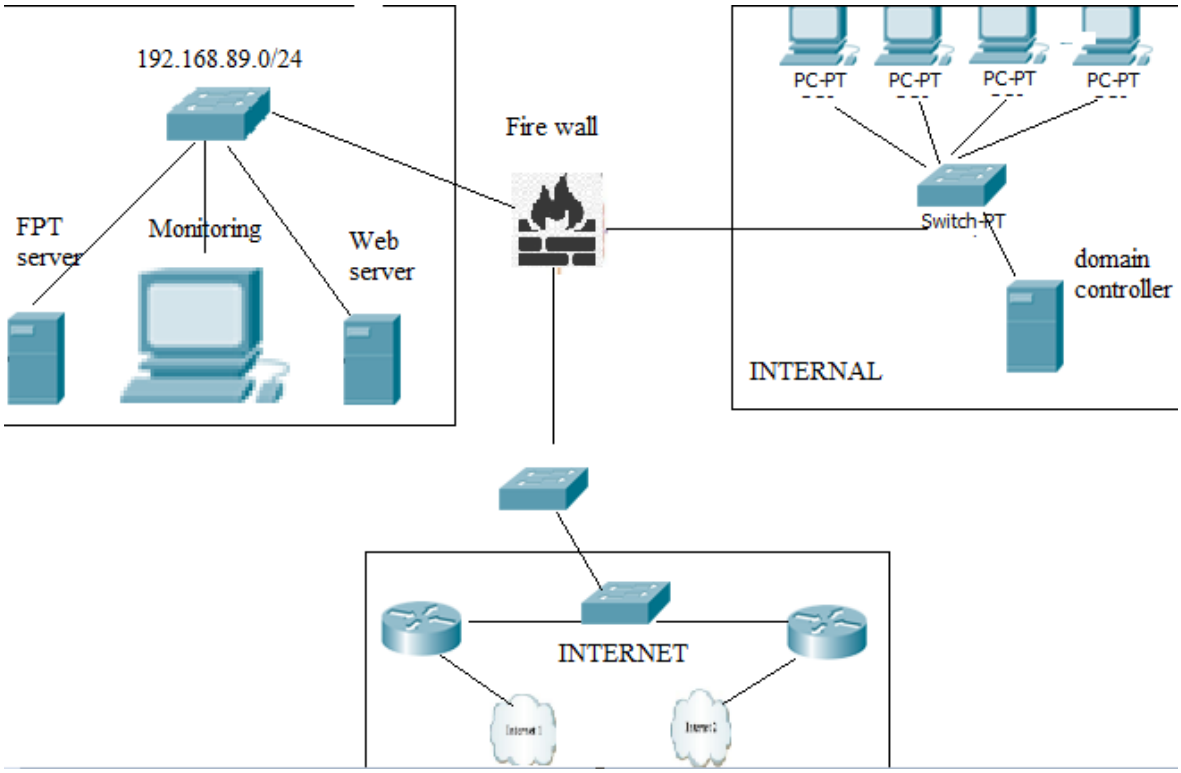
Hình 2-8: Trạng thái giám sát service

CHƯƠNG 3: ỨNG DỤNG THỰC NGHIỆM

3.1 Phát biểu bài toán

Mô phỏng hệ thống giám sát cho công ty Datatech bao gồm các văn phòng, các dây chuyền sản xuất, phòng thí nghiệm... Tất cả các phòng đều được trang bị các hệ thống máy tính phục vụ công việc sản xuất. Yêu cầu cài đặt server giám sát tự động các máy tính, tài nguyên hoạt động. Khi gặp sự cố hệ thống sẽ tự động thông báo đến các quản trị viên bằng email.

3.2 Cài đặt triển khai



Hình 3-1: Mô hình hệ thống giám sát Nagios

3.2.1 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 clinet 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: Là vùng cung cấp dịch vụ Internet cho người sử dụng trong công ty.

3.2.2 Triển khai hệ thống thực nghiệm

Hệ thống Nagios bắt đầu được cài đặt và giám sát những dịch vụ đầu tiên vào ngày 29/11/2019 trên server có địa chỉ mạng là 192.168.89.128. Địa chỉ truy cập vào hệ thống là http://192.168.89.128/nagios. Với mục đích thử nghiệm việc giám sát theo dõi các thiết bị, máy tính của công ty và gửi kết quả về cho server có địa chỉ là 192.168.89.128.

Các thành phần hệ thống mạng bao gồm:

STT	Host name	IP	OS	NOTE
1.	Nagiossver	192.168.89.128	Centos 6.10	Máy chủ giám sát thiết bị mạng , chương trình ứng dụng, tài nguyên các máy server khác
2.	Mail server	192.168.89.137	Centos 6.10	Thông báo tình trạng các dịch vụ của nagios server qua mail cho người dùng
3.	Web server	192.168.89.138	Windows Server 2008	Máy chủ dịch vụ web trên server
4.	Client	192.168.89.134,...	Windows 7	Các máy tính công ty

Xây dựng kịch bản giám sát các thiết bị, máy tính của công ty và thông báo về máy chủ nagios server gồm: 2 máy chủ chạy hệ điều hành server linux (Centos 6.10) và các máy tính được giám sát chạy trên hệ điều hành window7.

a). Giám sát trạng thái một số host

- Trạng thái hoạt động của host
- Trạng thái hoạt động của services

b). Giám sát việc sử dụng tài nguyên các máy window

- CPU số lượng processes trong hàng đợi hay 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.

c). Cảnh báo

- Cảnh báo trạng thái: Ví dụ máy clinet bị down bất thường, hay sự cố ngoài ý muốn
- Cảnh bảo dịch vụ: Services bị tắt hay thay đổi trạng thái

3.3 Thống kê tình trạng hoạt động của một số host/dịch vụ

Dưới đây là những số liệu ghi lại được về tình trạng hoạt động, độ ổn định của một số dịch vụ.

3.3.1 Server mail

3.3.1.1 Host mail

Bảng thông tin trạng thái và các thiết bị đặt cho giám sát server mail 192.168.89.137

Current Status:	OK (for 4d 15h 47m 45s)
Status Information:	OK - load average: 0.00, 0.02, 0.06
Performance Data:	load1=0.000;5.000;10.000;0; load5=0.020;4.000;6.000;0; load15=0.060;3.000;4.000;0;
Current Attempt:	1/4 (HARD state)
Last Check Time:	12-03-2019 18:56:20
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 0.009 seconds
Next Scheduled Check:	12-03-2019 19:01:20
Last State Change:	11-29-2019 03:13:20
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	12-03-2019 19:00:58 (0d 0h 0m 7s ago)

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

Hình 3-2: Thông tin mail server

Từ bảng trên ta có được các thông tin cơ bản về trạng thái host mail (server mail). Host mail đang ở trạng thái UP, lần kiểm tra cuối cùng cách đây bao lâu, loại kiểm tra (ACTIVE), host không bị flapping hay không, không được lập lịch downtime. Tất cả các tính năng đều được ENABLED.

Hình trên là bảng thống kê trạng thái của host mail từ 11-29-2019 đến 12-03-2019. Từ bảng này cho thấy host mail ở trạng thái UP(hoạt động) liên tục trong quãng thời gian được giám soát. Không có sự cố nào với host mail.

client	C:\ Drive Space	OK	12-09-2019 01:25:40	0d 2h 15m 36s	1/3	c: - total: 40.00 Gb - used: 7.43 Gb (19%) - free 32.57 Gb (81%)
	CPU Load	OK	12-09-2019 01:26:55	0d 2h 14m 21s	1/3	CPU Load 1% (5 min average)
	Explorer	OK	12-09-2019 01:28:10	0d 2h 13m 5s	1/3	explorer.exe: Running
	Memory Usage	OK	12-08-2019 23:37:19	0d 2h 21m 51s	1/3	Memory usage: total:1535.51 MB - used: 352.39 MB (23%) - free: 1183.12 MB (77%)
	NSClient++ Version	OK	12-08-2019 23:38:33	0d 2h 20m 37s	1/3	NSClient++ 0,4,1,90 2013-02-04
	Uptime	OK	12-08-2019 23:39:49	0d 2h 19m 21s	1/3	System Uptime - 0 day(s) 0 hour(s) 33 minute(s)
	W3SVC	CRITICAL	12-08-2019 23:37:04	5d 20h 38m 44s	3/3	W3SVC: Not found
localhost	Current Load	OK	12-09-2019 01:26:05	5d 20h 55m 34s	1/4	OK - load average: 0.35, 0.15, 0.05
	Current Users	OK	12-09-2019 01:27:20	5d 20h 54m 56s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	12-09-2019 01:28:35	2d 3h 8m 16s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 5159 bytes in 0.004 second response time
	PING	OK	12-09-2019 01:24:28	5d 20h 53m 41s	1/4	PING OK - Packet loss = 0%, RTA = 0.04 ms
	Root Partition	OK	12-09-2019 01:26:21	5d 20h 53m 4s	1/4	DISK OK - free space: / 14002 MB (83% inode=90%):
	SSH	OK	12-09-2019 01:26:17	5d 20h 52m 26s	1/4	SSH OK - OpenSSH_5.3 (protocol 2.0)
	Swap Usage	OK	12-09-2019 01:26:59	5d 20h 51m 49s	1/4	SWAP OK - 100% free (2047 MB out of 2047 MB)
	Total Processes	OK	12-09-2019 01:26:30	5d 20h 51m 11s	1/4	PROCS OK: 175 processes with STATE = RSZDT

Hình 3-3: Một số host được mail server kiểm soát

Bảng này cung cấp thông tin các máy tính window và linux, trạng thái hiện thời, lần kiểm tra cuối...

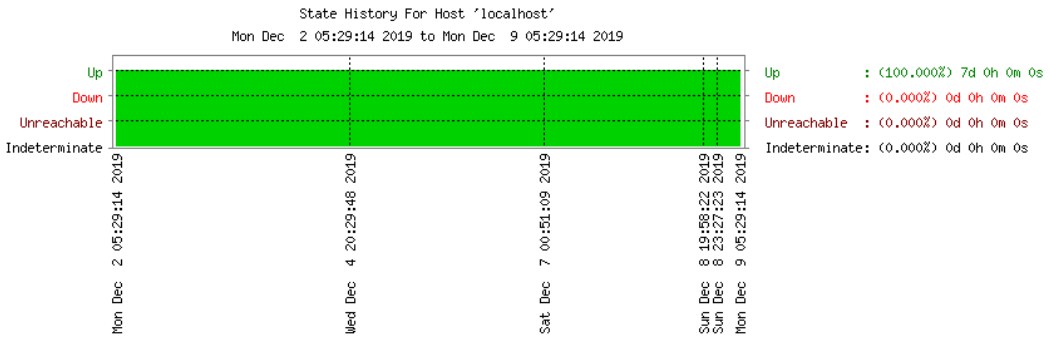
3.3.2 Giám sát máy tính linux

Các dịch vụ đã triển khai thử nghiệm trên máy sử dụng hệ điều hành linux là tình trạng sử dụng lượt tải, giám sát tổng số trình đang chạy, số người dùng hiện thời đang sử dụng các dịch vụ đang chạy.

localhost	Current Load	OK	12-09-2019 05:20:27	6d 0h 50m 36s	1/4	OK - load average: 0.39, 0.32, 0.14
	Current Users	OK	12-09-2019 05:21:42	6d 0h 49m 58s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	12-09-2019 05:22:57	2d 7h 3m 18s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 5159 bytes in 0.002 second response time
	PING	OK	12-09-2019 05:23:26	6d 0h 48m 43s	1/4	PING OK - Packet loss = 0%, RTA = 0.08 ms
	Root Partition	OK	12-09-2019 05:19:28	6d 0h 48m 6s	1/4	DISK OK - free space: / 14002 MB (83% inode=90%):
	SSH	OK	12-09-2019 05:22:23	6d 0h 47m 28s	1/4	SSH OK - OpenSSH_5.3 (protocol 2.0)
	Swap Usage	OK	12-09-2019 05:21:57	6d 0h 46m 51s	1/4	SWAP OK - 100% free (2047 MB out of 2047 MB)
	Total Processes	OK	12-09-2019 05:20:52	6d 0h 46m 13s	1/4	PROCS OK: 175 processes with STATE = RSZDT

Hình 3-4: Các dịch vụ được giám sát trên máy linux

Đây là số liệu trên hình 3.4 ghi lại hoạt động của máy linux trên server mail trong tháng 12-2019. Ghi lại các trạng thái dừng hoạt động, khôi phục, cảnh báo, không xác định của dịch vụ (UP, DOWN, UNREACHABLE, INDETERMINATE) của dịch vụ. Cột dọc là các trạng thái, cột ngang là thời gian. Bên phải là thống kê các trạng thái theo phần trăm.

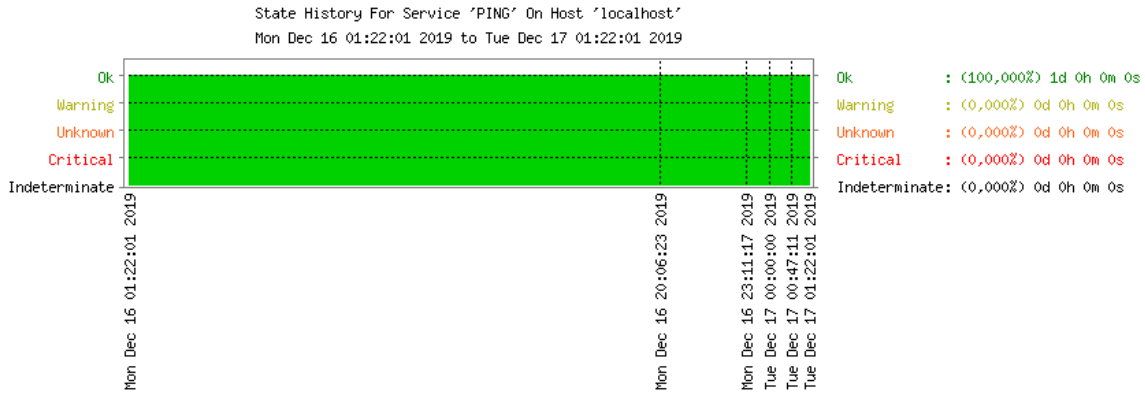


Hình 3-5: Số liệu hoạt động của máy linux

Từ số liệu trên hình 3-5 chúng ta có thể thấy trong tháng 12-2019, máy tính linux của chúng ta sử dụng rất ổn định không ngày nào bị DOWN. Đây là số liệu ngày 02/12/2019 đến 09/12/2019.

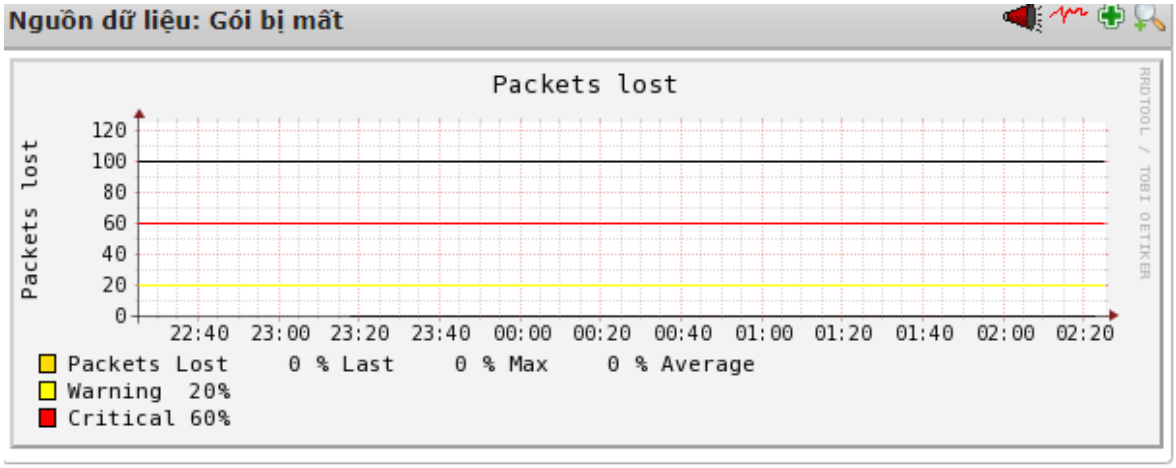
3.3.2.1 Một số dịch vụ được dùng trên máy linux

a). Dịch vụ PING



Hình 3-6: Tình trạng hoạt động của PING

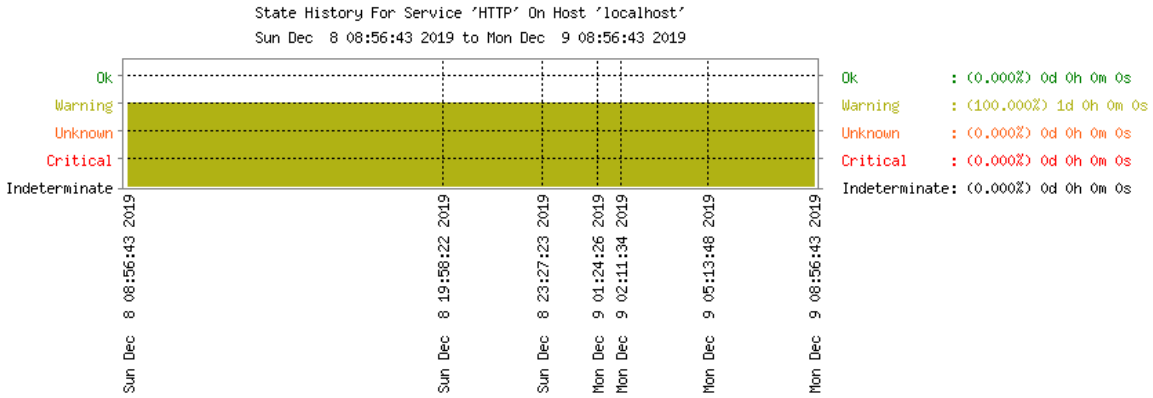
Đây là số liệu ghi lại hoạt động của dịch vụ PING từ ngày 16/12/2019-17/12/2019. Ghi lại các trạng thái dừng hoạt động, khôi phục, cảnh báo, không xác định của dịch vụ (OK, WARNING, CRITICAL, UNKNOWN) của dịch vụ. Cột ngang là các trạng thái, cột dọc là thời gian. Bên phải thống kê các trạng thái theo phần trăm.



Hình 3-7: Biểu đồ dịch vụ PING

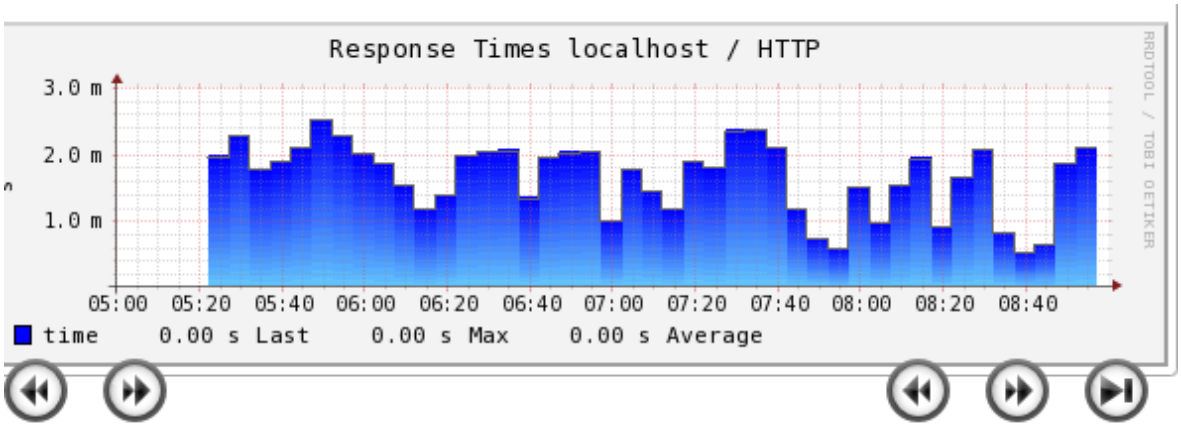
Qua biểu đồ này nhằm giúp chúng ta biết được mạng không bị xâm nhập và các gói được trả lại cho người gửi một cách an toàn. Tất cả mọi thứ hiện tại vẫn đang trong tình trạng được kiểm soát.

b). Dịch vụ HTTP (server web)



Hình 3-8: Tình trạng hoạt động của HTTP

Đây là số liệu của dịch vụ HTTP có thể do quá nhiều lượt truy cập vào server web nên đã gặp phải tình trạng Warning.



Hình 3-9: Biểu đồ HTTP

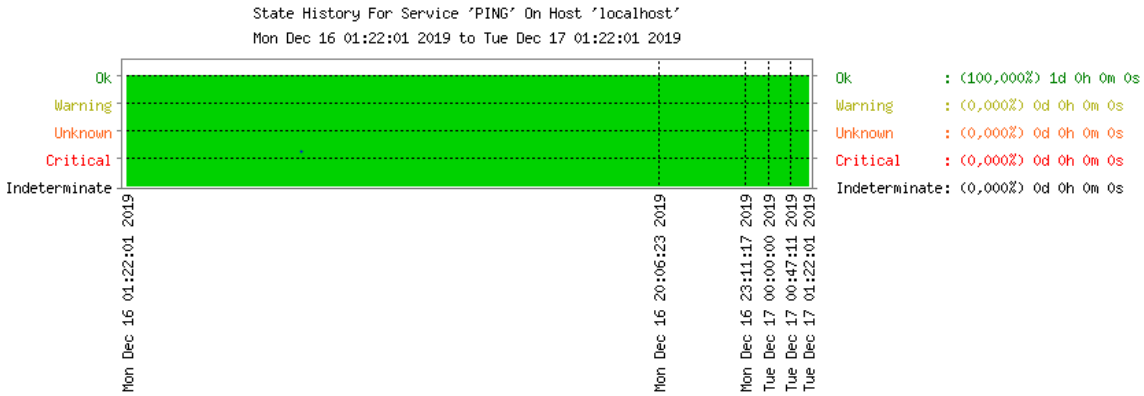
Như chúng ta quan sát biểu đồ có thể do dịch vụ của HTTP không ổn định lên đã dẫn đến tình trạng Warning. Thông báo tình trạng dịch vụ HTTP đang ở trạng thái nguy hiểm được gửi đến cho người quản trị qua email. Khuôn dạng thông báo có dạng kiểu như sau:

```
***** Nagios *****

Notification Type: PROBLEM

Service: HTTP
Host: localhost
Address: 192.168.89.128
State: WARNING

Date/Time: Sun Dec 19 22:08:40 PST 2019
```

Hình 3-10: Nội dung email cảnh báo dịch vụ HTTP đang WARNING

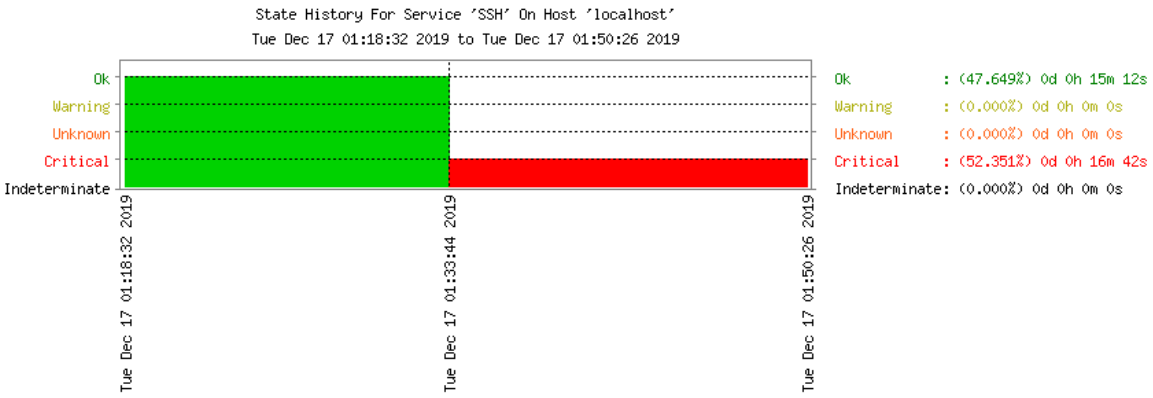
c). Dịch vụ SSH

Ở phần này chúng ta sẽ thực hiện phần cảnh báo dịch vụ SSH thay đổi trạng thái.



Hình 3-11: Tình trạng hoạt động SSH đang ổn định

Ở hình 3.11 có thể thấy dịch vụ SSH đang hoạt động bình thường từ 16:01' ngày 16/12/2019 – 01:22' ngày 17/12/2019. Bây giờ chúng ta sẽ thực hiện can thiệp vào SSH bằng câu lệnh: 'service sshd stop' để dừng dịch vụ lại.



Hình 3-12: Dịch vụ SSH bị tắt

Khi chúng ta can thiệp dừng dịch vụ SSH sẽ hiện nên khoảng trống màu đỏ thể hiện tình trạng Critical, đồng thực email sẽ gửi đến quản trị viên về tình trạng dịch vụ SSH bị thay đổi đột ngột.

```
***** Nagios *****

Notification Type: PROBLEM

Service: SSH
Host: localhost
Address: 192.168.89.128
State: CRITICAL

Date/Time: Tue Dec 17 1:55:40 PST 2019
```

Hình 3-13: Nội dung email cảnh báo dịch vụ SSH đang CRITICAL

Hình chụp 1 số cảnh báo được đưa ra và được ghi lại trong tệp log. Cảnh báo OK là ghi nhận dịch vụ trở lại hoạt động. Cảnh báo hình CRITICAL là dịch vụ dừng hoạt động.

Service Log Entries:

[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
11-11-2019 00:00:00	11-11-2019 04:30:38	0d 4h 30m 38s	SERVICE OK (HARD)	SSH OK - OpenSSH_5.3 (protocol 2.0)
12-17-2019 00:00:00	12-17-2019 00:47:11	0d 0h 47m 11s	SERVICE OK (HARD)	SSH OK - OpenSSH_5.3 (protocol 2.0)
12-17-2019 01:33:44	12-17-2019 02:11:17	0d 0h 37m 33s+	SERVICE CRITICAL (HARD)	connect to address 127.0.0.1 and port 22: Connection refused

Hình 3-14: Log thông báo

3.3.3 Giám sát máy tính window server 2k8

Các dịch vụ đã triển khai thử nghiệm trên máy sử dụng hệ điều hành Window server 2k8 là tình trạng sử dụng CPU, ổ đĩa cứng, RAM, giám sát hoạt động các tiến trình, các dịch vụ đang chạy.

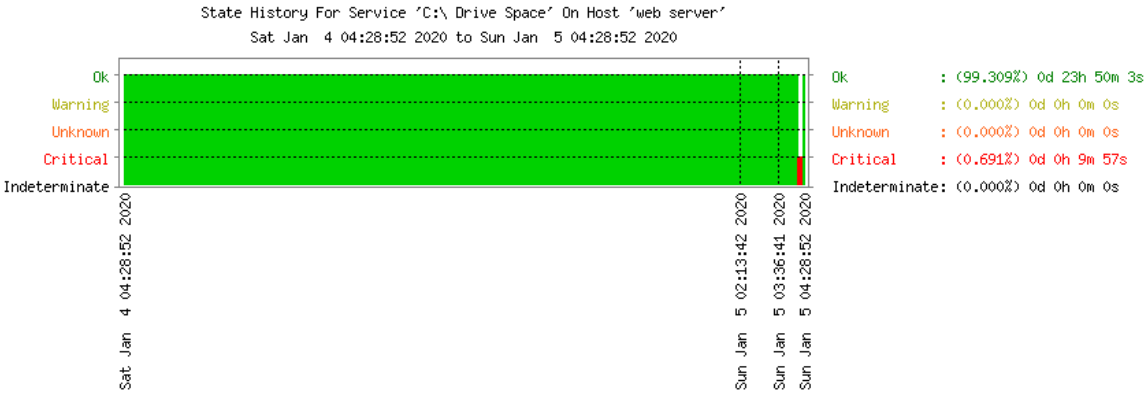
web server	C:\ Drive Space		OK	01-05-2020 04:26:09	0d 0h 9m 39s	1/3	c: - total: 40.00 Gb - used: 7.23 Gb (18%) - free 32.77 Gb (82%)
	CPU Load		OK	01-05-2020 04:29:27	0d 0h 6m 21s	1/3	CPU Load 2% (5 min average)
	Explorer		OK	01-05-2020 04:33:58	0d 0h 1m 50s	1/3	explorer.exe: Running
	HTTP		WARNING	01-05-2020 04:27:16	0d 0h 8m 32s	3/3	HTTP WARNING: HTTP/1.1 404 Not Found - 492 bytes in 0.014 second response time
	Memory Usage		OK	01-05-2020 04:32:34	0d 0h 3m 14s	1/3	Memory usage: total:1503.26 MB - used: 384.27 MB (26%) - free: 1118.99 MB (74%)
	Uptime		OK	01-05-2020 04:33:53	0d 0h 11m 55s	1/3	System Uptime - 0 day(s) 0 hour(s) 10 minute(s)
	W3SVC		OK	01-05-2020 04:29:11	0d 0h 6m 37s	1/3	W3SVC: Started

Hình 3-15: Các dịch vụ được giám sát trên window server 2k8

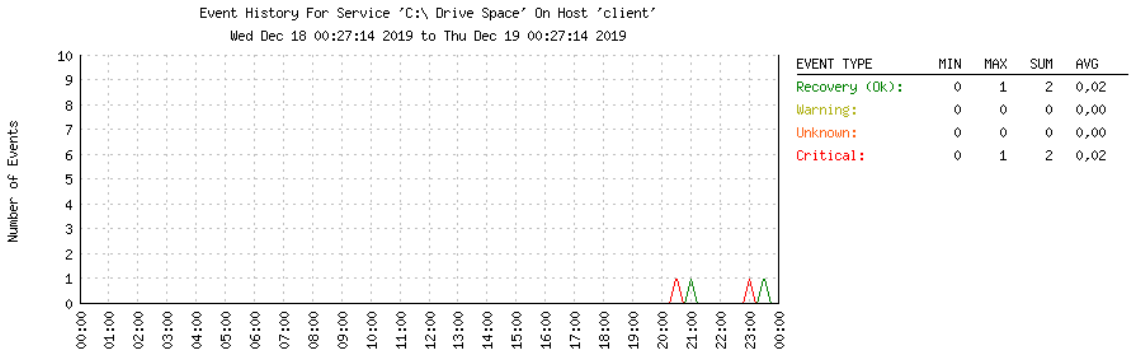
3.3.3.1 Một số dịch vụ được sử dung giám sát

a). Tài nguyên ổ cứng

Đây là số liệu của ổ đĩa cứng trên thiết bị window từ ngày 04/01/2020 đến 05/01/2020. Trong đó chỉ ghi nhận một lần ổ đĩa cứng không dùng được từ 03h36’ đến 04h28’ ngày 05/01/2020.



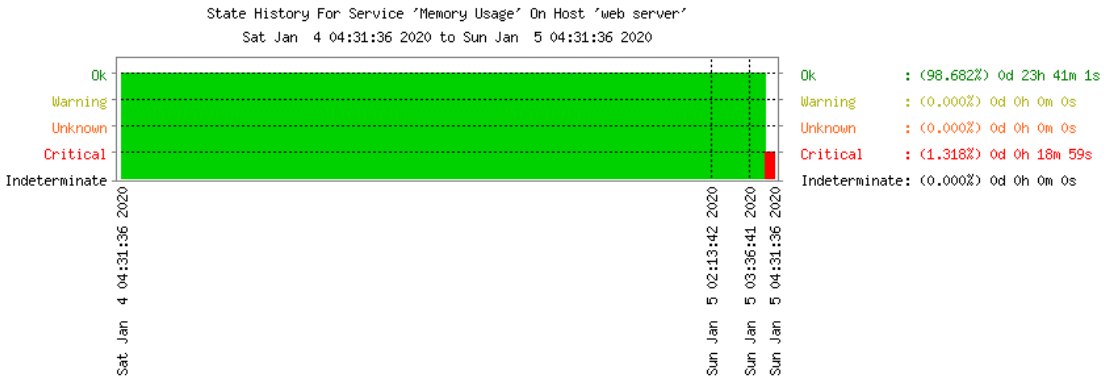
Hình 3-16: Diễn biến hoạt động của ổ cứng



Hình 3-17: Biểu đồ sử dụng ổ cứng

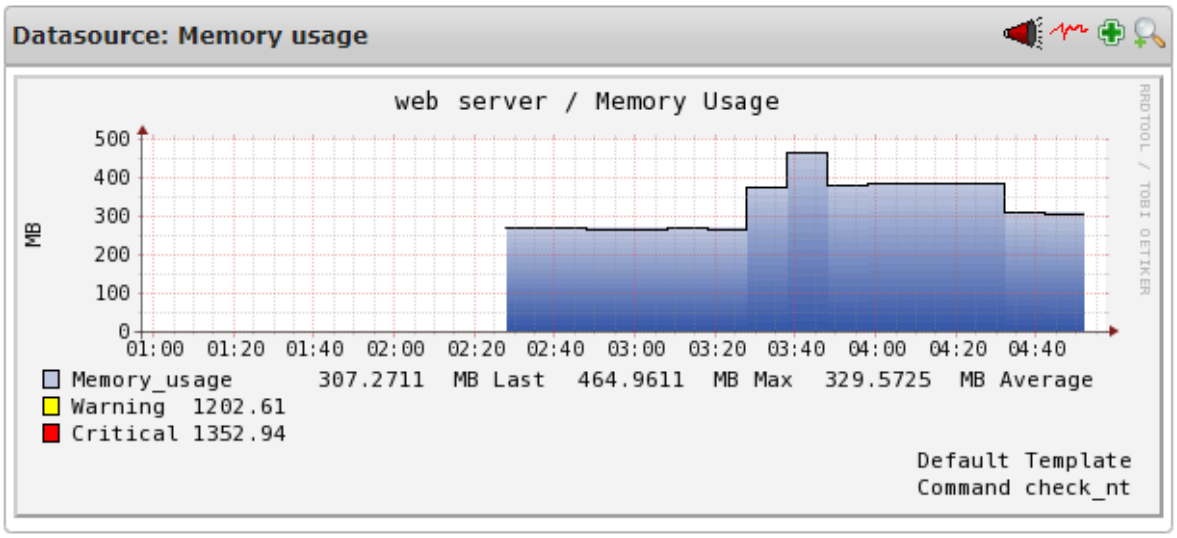
Trên hình 3.17 chúng ta có thể thấy màu xanh là khoảng thời gian ổ cứng sử dụng bình thường có màu xanh còn màu đỏ chỉ định ổ cứng đang có vấn đề.

b.) Tài nguyên RAM



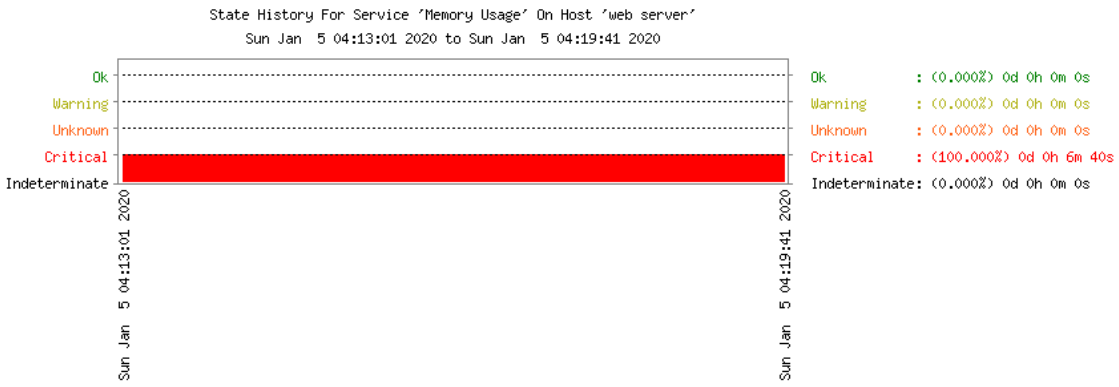
Hình 3-18: Diễn biến hoạt động của RAM

Đây là số liệu của RAM trên thiết bị window từ ngày 04/01/2020 đến 05/01/2020. Trong đó chỉ ghi nhận một lần RAM không dùng được từ 03h36' đến 04h31' ngày 05/01/2020.



Hình 3-19: Biểu đồ sử dụng RAM

Dựa vào biểu đồ trên chúng ta có thể quan sát được thông số sử dụng RAM của máy window 464MB/2GB



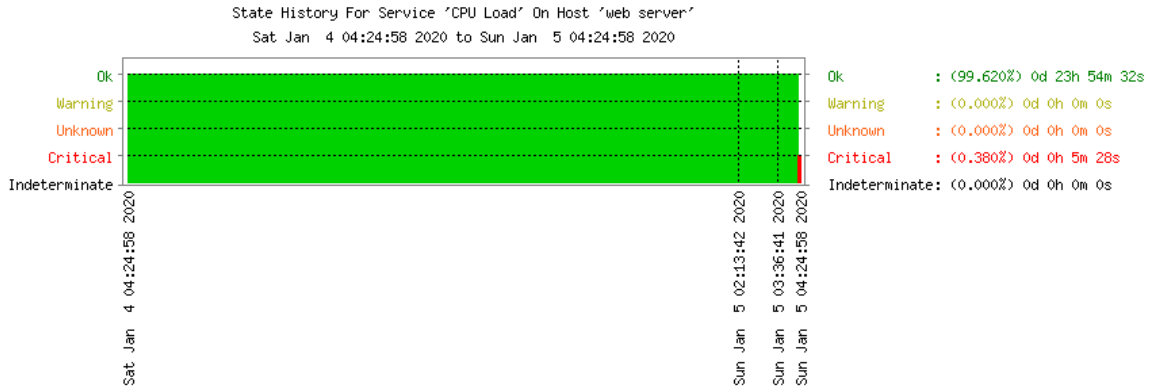
Hình 3-20: RAM đang bị quá tải

Đây là khoảng thời gian máy tính đang hoạt động liên tiếp nhiều giờ và có nhiều chu trình ở trạng thái chờ sẽ dẫn đến tình trạng RAM bị quá tải. Đồng thời khi RAM bị quá tải chúng ta sẽ được nhận 1 email thông báo đến quản trị viên để kiểm soát.

```
***** Nagios *****

Service: Memory Usage
Notification Type: PROBLEM
Host: web server
Address: 192.168.89.138
State: CRITICAL

Date/Time: Sat Jan 5 04:33:09 PST 2020
```

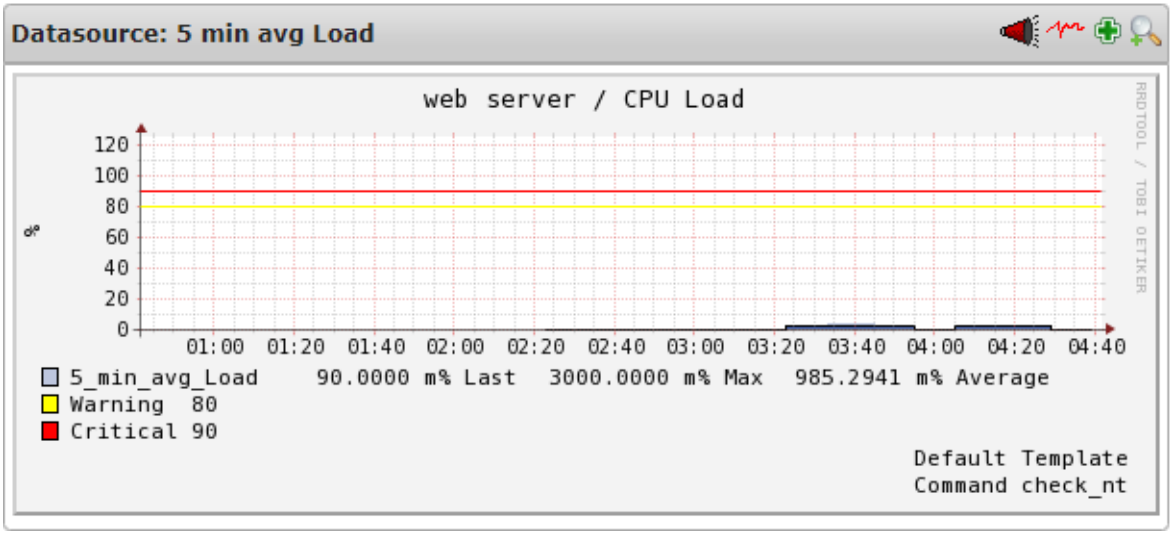
Hình 3-21: Email cảnh báo RAM đang quá tải

c). Tài nguyên CPU



Hình 3-22: Diễn biến hoạt động của CPU

Đây là số liệu của CPU trên thiết bị window từ ngày 04/01/2019 đến 05/01/2020. Trong đó chỉ ghi nhận một lần CPU không dùng được từ 03h36’ đến 04h24’ ngày 05/01/2020.



Hình 3-23: Biểu đồ sử dụng CPU

Theo dõi CPU của máy, quản trị viên sẽ được nhận cảnh báo đến email CRITICAL nếu CPU quả tải 5 phút 80% trở nên hoặc WARNING nếu CPU hoạt động đến 70%.

```
***** Nagios *****

Service: CPU
Notification Type: PROBLEM
Host: web server
Address: 192.168.89.138
State: CRITICAL

Date/Time: Sat Jan 5 04:24:17 PST 2020
```

Hình 3-24: Email về tình trạng CPU

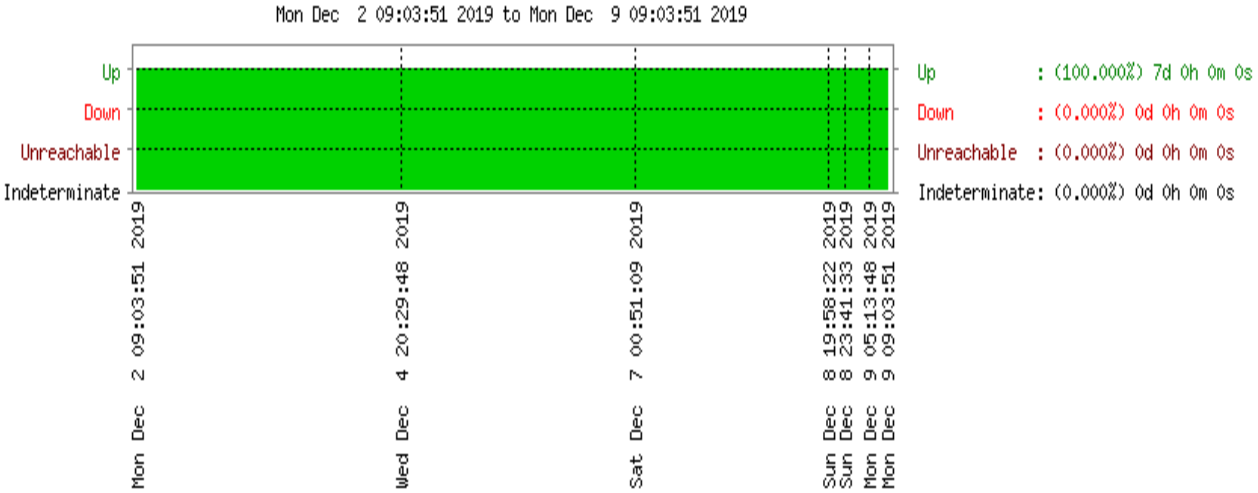
d.) Cảnh báo sự cố

Từ những thông tin trên chúng ta có thể thấy ngày 05/01/2020 máy tính window server 2k8 của chúng ta đã gặp sự cố bị down trạng thái sẽ được gửi đến cho người quản trị email. Khuôn dạng thông báo có dạng kiểu như sau:

```
***** Nagios *****

Notification Type: PROBLEM

Host: web server
Address: 192.168.89.138
State: DOWN

Date/Time: Sat Jan 5 04:38:22 PST 2020
```

Hình 3-25: Nội dung email

3.3.4 Một số nhận định về Nagios



Hình 3-26: Tình trạng hoạt động của Nagios từ 02/12/2019 đến 09/12/2019

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 thộng 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://vi.wikipedia.org/wiki/Trang_Ch%C3%ADnh

[2]. https://adminvietnam.org/nagios-tren-centos-6/121/

[3]. https://www.nagios.com/ trang chủ tài liệu nagios hỗ trợ người dùng

[4].https://hvazone.com/monitoring-with-nagios-luan-nghien-cuu-cua-tg-pham-hong-khai.1531.html

[5]. Essential SNMP / Douglas R. Mauro and Kevin J. Schmidt

[6]. SMNP toàn tập – Nguyễn Thanh Diệp

[7].https://lib.hpu.edu.vn/bitstream/handle/123456789/32916/Hoang-Van-Can-CT1802.pdf?sequence=1&isAllowed=y