**ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**



**Trương Xuân Hội**

**XÂY DỰNG HỆ THỐNG GIÁM SÁT VÀ CẢNH BÁO  
DỰA TRÊN GIAO THỨC SNMP  
CHO ĐẠI HỌC CÔNG NGHỆ**

**ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY  
Ngành: Truyền thông và mạng máy tính**

**Hà Nội – 2020**

**ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**Trương Xuân Hội**

**XÂY DỰNG HỆ THỐNG GIÁM SÁT VÀ CẢNH BÁO  
DỰA TRÊN GIAO THỨC SNMP  
CHO ĐẠI HỌC CÔNG NGHỆ**

**ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY  
Ngành: Truyền thông và mạng máy tính**

**Cán bộ hướng dẫn: Ths. Đỗ Hoàng Kiên**

**Hà Nội – 2020**

**TÓM TẮT**

Cùng với sự phát triển của công nghệ thông tin, sự đầu tư cho hạ tầng mạng trong mỗi doanh nghiệp ngày càng tăng cao, dẫn đến việc quản trị sự cố một hệ thống mạng gặp rất nhiều khó khăn. Đi cùng với những lợi ích khi phát triển hạ tầng mạng như băng thông cao, khối lượng dữ liệu trong mạng lớn, đáp ứng được nhu cầu của người dùng, hệ thống mạng phải đối đầu với rất nhiều thách thức như các cuộc tấn công bên ngoài, tính sẵn sàng của thiết bị, tài nguyên của hệ thống, …

Một trong những giải pháp hữu hiệu nhất để giải quyết vấn đề này là thực hiện giải pháp giám sát mạng, dựa trên những thông tin thu thập được thông qua quá trình giám sát, các nhân viên quản trị mạng có thể phân tích, đưa ra những đánh giá, dự báo, giải pháp nhằm giải quyết những vấn đề trên. Để thực hiện giám sát mạng có hiệu quả, một chương trình giám sát phải đáp ứng được các yêu cầu sau: phải đảm bảo chương trình luôn hoạt động, tính linh hoạt, chức năng hiệu quả, đơn giản trong triển khai, chi phí thấp. Hiện nay, có khá nhiều phần mềm hỗ trợ việc giám sát có hiệu quả như Nagios, Zabbix, Zenoss, Cacti, …

Vì vậy, em chọn đề tài “**Xây dựng hệ thống giám sát và cảnh báo dựa trên giao thức SNMP cho đại học Công Nghệ**” sử dụng phần mềm mã nguồn mở Zabbix. Với mục tiêu nghiên cứu, tìm hiểu về giải pháp giúp cho mọi người có cái nhìn tổng quan về hệ thống giám sát mạng hoàn chỉnh, đồng thời đưa ra giải pháp cụ thể đối với một hệ thống mạng dành cho doanh nghiệp.

**LỜI CAM ĐOAN**

Em xin cam đoan không sao chép tài liệu, công trình nghiên cứu của người khác mà không chỉ rõ trong tài liệu tham khảo.

Hà Nội, ngày tháng năm

Sinh viên

Trương Xuân Hội

**MỤC LỤC**

[LỜI MỞ ĐẦU 1](#_Toc52554515)

[CHƯƠNG 1. TỔNG QUAN VỀ GIÁM SÁT MẠNG 2](#_Toc52554516)

[1.1. Định nghĩa về giám sát mạng 2](#_Toc52554517)

[1.1.1. Định nghĩa 2](#_Toc52554518)

[1.1.2. Các yếu tố cơ bản trong giám sát mạng 2](#_Toc52554519)

[1.1.3. Cách thức giám sát mạng 2](#_Toc52554520)

[1.1.4. Tầm quan trọng của giám sát mạng 3](#_Toc52554521)

[1.2. Thực trạng hệ thống mạng ở Việt Nam hiện nay 4](#_Toc52554522)

[1.2.1. Yếu tố phần cứng 4](#_Toc52554523)

[1.2.2. Yếu tố phần mềm 5](#_Toc52554524)

[1.2.3. Yếu tố con người 6](#_Toc52554525)

[1.3. Tổng quan về các giao thức mạng 6](#_Toc52554526)

[1.3.1. Bộ giao thức TCP/IP 6](#_Toc52554527)

[1.3.2. Giao thức UDP 7](#_Toc52554528)

[1.3.3. So sánh giữa giao thức UDP và TCP 8](#_Toc52554529)

[1.3.4. Giao thức ICMP 9](#_Toc52554530)

[1.4. Các kỹ thuật và giao thức giám sát cơ bản 10](#_Toc52554531)

[1.5. Các quy tắc khi thiết kế hệ thống giám sát mạng 11](#_Toc52554532)

[1.5.1. Mô hình FCAPS (Fault Configuration Accounting Performance Security).................. 11](#_Toc52554533)

[1.5.2. Báo cáo và cảnh báo 12](#_Toc52554534)

[1.5.3. Một số thuật ngữ liên quan đến cảnh báo 13](#_Toc52554535)

[1.5.4. Tích hợp lưu trữ dữ liệu 13](#_Toc52554536)

[1.6. Các vấn đề trong giám sát mạng 13](#_Toc52554537)

[1.6.1. Giám sát khả dụng (Availability Monitoring) 14](#_Toc52554538)

[1.6.2. Giám sát giao diện (Interface Monitoring) 15](#_Toc52554539)

[1.6.3. Giám sát mức độ sử dụng ổ đĩa (Disk Monitoring) 15](#_Toc52554540)

[1.6.4. Giám sát phần cứng 15](#_Toc52554541)

[1.7. Tổng quan về giao thức SNMP 16](#_Toc52554542)

[1.7.1. Các thành phần cơ bản trong SNMP 16](#_Toc52554543)

[1.7.2. Chức năng của giao thức SNMP 18](#_Toc52554544)

[1.7.3. Sơ lược về Object Identifier (OID) 19](#_Toc52554545)

[1.7.4. Mối liên hệ giữa MIB và SNMP 19](#_Toc52554546)

[1.7.5. Khái niệm về chuỗi community 20](#_Toc52554547)

[1.7.6. Các thuật ngữ và cổng sử dụng trong SNMP 20](#_Toc52554548)

[1.7.7. Các phiên bản SNMP 21](#_Toc52554549)

[1.7.8. Giám sát hệ điều hành Windows bằng giao thức SNMP 21](#_Toc52554550)

[1.8. Các giải pháp và công cụ giám sát mạng phổ biến 23](#_Toc52554551)

[1.8.1. Các giải pháp giám sát mạng 23](#_Toc52554552)

[1.8.2. Một số công cụ giám sát mạng phổ biến 24](#_Toc52554553)

[CHƯƠNG 2. TÌM HIỂU VỀ PHẦN MỀM ZABBIX 25](#_Toc52554554)

[2.1. Kiến thức chung về phần mềm Zabbix 25](#_Toc52554555)

[2.1.1. Tổng quan........................................................................................25](#_Toc52554556)

[2.1.2. Các tính năng của Zabbix 26](#_Toc52554557)

[2.1.3. Các chức năng của Zabbix 27](#_Toc52554558)

[2.2. Ưu nhược điểm của Zabbix so với hệ thống giám sát phổ biến khác 29](#_Toc52554559)

[2.3. Kiến trúc của hệ thống giám sát Zabbix 31](#_Toc52554560)

[2.4. Cơ chế hoạt động 33](#_Toc52554561)

[2.5. Các mô hình triển khai hệ thống Zabbix 33](#_Toc52554562)

[2.6. Các thành phần cơ bản trong Zabbix 35](#_Toc52554563)

[CHƯƠNG 3. MÔ PHỎNG VÀ ĐÁNH GIÁ 35](#_Toc52554564)

[3.1. Sơ đồ mô phỏng 36](#_Toc52554565)

[3.2. Kỹ thuật sử dụng 37](#_Toc52554566)

[3.3. Thiết lập cảnh báo 42](#_Toc52554567)

[3.3.1. Cảnh báo tại máy 42](#_Toc52554568)

[3.3.2. Cảnh báo online 43](#_Toc52554569)

[3.4. Cảnh báo sự cố 49](#_Toc52554570)

[3.4.1. Cảnh báo trực tiếp trên màn hình chính 49](#_Toc52554571)

[3.4.2. Cảnh báo qua mail 49](#_Toc52554572)

[KẾT LUẬN 51](#_Toc52554573)

[TÀI LIỆU THAM KHẢO 52](#_Toc52554574)

# LỜI MỞ ĐẦU

1. **Sơ lược về đề tài**

* Thực hiện việc giám sát trạng thái các server và các dịch vụ chạy trên máy server.
* Thực hiện việc giám sát các trạng thái và lưu lượng trên các cổng switch và router.
* Thực hiện việc cảnh báo thông qua giao diện web, email và sms khi một host hoặc một dịch vụ down.

1. **Mục tiêu đề tài**

* Xem xét các giải pháp giám sát hệ thống mạng, theo dõi tình trạng hoạt động của các server, switch, router, và một số dịch vuh mạng.
* Phát triển hệ thống cảnh báo qua web và email.

1. **Đối tượng nghiên cứu**

* Phần mềm mã nguồn mở Zabbix dùng để giám sát các thiết bị mạng.
* Phần mềm giả lập mạng ảo EVE-NG

1. **Nội dung nghiên cứu**

* Nghiên cứu các giải pháp giám sát hoạt động của các thiết bị mạng.
* Nghiên cứu các giải pháp giám sát hoạt động dịch vụ trong hệ thống mạng: HTTP, FTP, …
* Đề xuất công cụ mã nguồn mở hỗ trợ giám sát hoạt động trên các thiết bị, dịch vụ mạng.
* Tìm hiểu về giao thức SNMP
* Xây dựng hệ thống cảnh báo.

# TỔNG QUAN VỀ GIÁM SÁT MẠNG

## Định nghĩa về giám sát mạng

### Định nghĩa

“Là việc giám sát mạng lưới máy tính liên tục, kiểm tra tốc độ truyền tải mạng và đưa ra các thông báo về trạng thái của hệ thống mạng cho quản trị viên (có thể qua mail, tin nhắn hoặc các hình thức khác)”. Đối tượng của giám sát mạng là tất cả các thành phần, thiết bị trong hệ thống mạng, bao gồm:

* Các máy trạm
* Cơ sở dữ liệu
* Các ứng dụng
* Các server
* Các thiết bị mạng
* Lưu lượng truyền tải mạng

Giám sát là một phần trong quản trị mạng. Công việc này thường được thực hiện qua các phần mềm hay công cụ. Những dịch vụ giám sát mạng được sử dụng khá nhiều trong việc nhận biết máy chủ hoặc các thiết bị mạng nào đó đang hoạt động và đã kết nối với mạng toàn cầu.

### 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.

### Cách thức giám sát mạng

Hệ thống giám sát mạng có thể giám sát các vấn đề về mạng như máy chủ bị quá tải hay bị sập, ngoài ra còn kiểm tra các kết nối mạng và các thiết bị khác. Hệ thống giám sát có thể dò và đưa ra các thông số mạng, những thông số này bao gồm lượng dữ liệu truyền tải, số lỗi, downtime/uptime, thời gian sử dụng và phản hồi đến người dùng. Khi ngưỡng của các tham số đạt mức giới hạn, hệ thống cảnh báo sẽ được kích hoạt và quản trị viên sẽ biết được hệ thống đang bị lỗi ở đâu và kịp thời đưa ra phương pháp xử lý hiệu quả.

### Tầm quan trọng của giám sát mạng

Giám sát mạng thực sự là việc rất cần thiết trong công việc. Không chỉ bởi tính an toàn và bảo mật dữ liệu, giám sát mạng có thể giúp doanh nghiệp tiết kiệm chi phí sửa chữa, giảm thiểu thời gian chết của hệ thống khi gặp sự cố, đảm bảo tính thông suốt trong toàn hệ thống. Những tiêu chí dưới đây sẽ giải thích rõ hơn vì sao giám sát mạng lại là một phần quan trọng đối với các doanh nghiệp:

* Tính bảo mật: Đảm bảo các thông tin không bị lộ ra ngoài. Là một trong những phần quan trọng của 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 nào có sự cố 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 là một trong những lợi thế của giám sát mạng. Tiết kiệm thời gian chẩn 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 người 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 được tìm ra và xử lý hiệu quả, có thể tập trung nhiều 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.

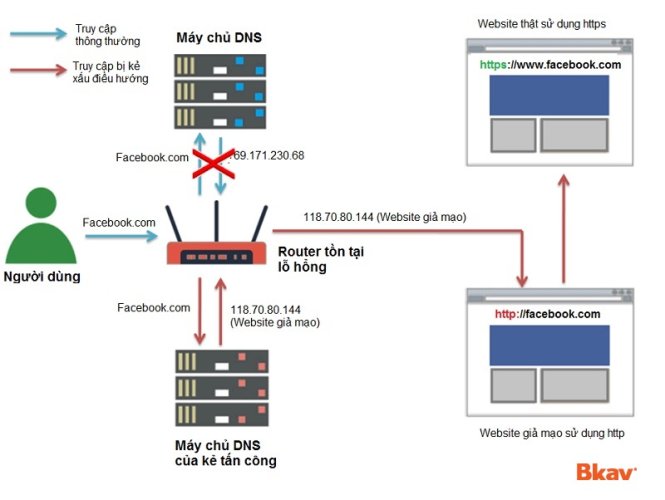
## Thực trạng hệ thống mạng ở Việt Nam hiện nay

Hệ thống mạng của Việt Nam hiện nay rất dễ bị tấn công, các nguyên nhân phải đề cập đến là hệ thống bảo mật thông tin chưa được đầu tư đồng bộ, thiếu nhân lực có năng lực chuyên môn và giải pháp xử lý chưa hiệu quả. Những nguyên nhân trên có thể đưa vào 3 yếu tố chính sau:

* Yếu tố phần cứng
* Yếu tố phần mềm
* Yếu tố con người

### Yếu tố phần cứng

Phần cứng là một trong các yếu tố ảnh hưởng đến độ an toàn của hệ thống mạng. Do cơ sở hạ tầng mạng thiếu sự đồng bộ, các doanh nghiệp nhỏ và vừa sử dụng các thiết bị có giá thành thấp, không rõ nguồn gốc để tiết kiệm chi phí cũng là nguyên nhân đưa hệ thống vào vùng nguy hiểm. Nghiên cứu của Bkav trong năm 2016 chỉ ra rằng: “Việt Nam thuộc top 5 quốc gia có số router bị lỗ hổng nhiều nhất, với số router là 300.000, tương đương với 300.000 hệ thống mạng có khả năng bị hacker chiếm quyền kiểm soát. Hơn 90% các router có lỗ hổng có xuất xứ từ Trung Quốc. Bkav cho biết lỗ hổng này nguy hiểm hơn Heartbleed – một trong những lỗ hổng bảo mật lớn nhất trong lịch sử Internet. Bởi vì Heartbleed cần người có trình độ chuyên gia an ninh mới có thể khai thác thành công, còn với lỗ hổng trên router không cần quá nhiều kiến thức về kĩ thuật”.



***Hình 1.1. Mô hình tấn công thông qua khai thác Pet Hole***

Vậy nên, để tránh bị tin tặc tấn công, các doanh nghiệp cần chú trọng đầu tư vào các thiết bị mạng chuẩn, có nguồn gốc rõ ràng như Cisco hay IBM, và chỉ nên dùng một hãng sản xuất nhằm tránh những xung đột không đáng có.

### Yếu tố phần mềm

Theo thống kê của Bkav năm 2016: “Trung bình mỗi tháng ở Việt Nam có 300 trang web của tổ chức, doanh nghiệp bị hacker tấn công và 40% trang web trong nước tồn tại lỗ hổng bảo mật. Việt Nam cũng nằm trong danh sách quốc gia có tỷ lệ lây nhiễm phần mềm độc hại cao nhất thế giới là 66%, tỷ lệ người dùng phải đối mặt với các mối đe dọa từ trang web là 35% - đứng thứ 3 thế giới sau Nga và Trung Quốc theo đánh giá của Karpersky Lab”. Nguyên do chính là bởi người dùng tải và cài đặt phần mềm có cài mã độc mà bản thân không hề hay biết. Các hacker lợi dụng tính tò mò và ưa chuộng các sản phẩm miễn phí của một số người dùng, đã lén đưa mã độc vào trong file cài đặt phần mềm hoặc đường liên kết, một khi người sử dụng kích hoạt, máy tính ngay lập tức sẽ bị nhiễm virus và họ chỉ phát hiện ra khi dữ liệu trong máy tự nhiên biến mất. Một nguyên nhân khác, là do không có sự thống nhất trong việc sử dụng phần mềm bảo mật, dẫn đến xung đột và tạo ra lỗ hổng.

Vì vậy, các doanh nghiệp cần đưa ra những chính sách về quản lý phần mềm, sử dụng các phầm mềm có bản quyền chính thống, không cho phép người dùng trong công ty tải về máy tính các phần mềm không rõ nguồn gốc. Sử dụng chung một phần mềm bảo mật của bên thứ ba như Kaspersky hay Avast cho tất cả máy tính trong công ty để tránh xung đột.

### Yếu tố con người

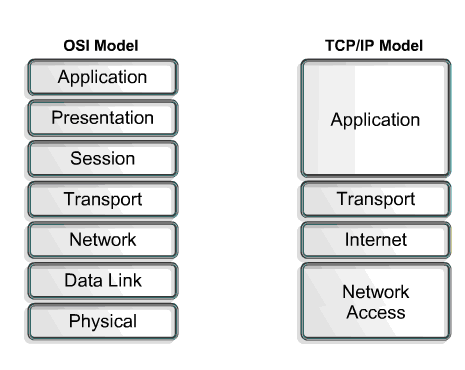
Bản thân người dùng không có kiến thức căn bản về bảo mật, tạo điều kiện để tin tặc tấn công. Người Việt Nam vốn thích sử dụng các phần mềm miễn phí , phần mềm crack bởi họ không có tiền để mua bản chính thống, chính điều này đã làm gia tăng nguy cơ nhiễm virus cho máy tính của họ, chưa kể đến, nếu họ sử dụng máy của công ty để tải về thì sẽ không biết có bao nhiêu máy khác trong công ty đó cũng sẽ bị nhiễm. Ngoài ra, do trình độ quản trị viên còn kém, hệ thống bảo mật lỏng lẻo, không tìm ra cách khắc phục dẫn đến việc toàn bộ hệ thống mạng trong công ty bị tin tặc chiếm quyền kiểm soát, điển hình là vụ sân bay Tân Sơn Nhất bị 2 em học sinh lớp 9 đột nhập vào hệ thống khiến cho khách hàng không đặt được vé năm 2017 (*VNExpress 2017. Website sân bay Tân Sơn Nhất bị tin tặc tấn công*) và một vụ do tin tặc Trung Quốc tấn công năm 2016.

Vì vậy, để tránh các trường hợp như trên xảy ra, các doanh nghiệp cần tuyển chọn những người có trình độ chuyên môn cao về hệ thống mạng, cử người đi đào tạo về mạng và tổ chức các đợt diễn tập phòng chống tấn công mạng thường niên nhằm nâng cao cảnh giác với tội phạm mạng.

## Tổng quan về các giao thức mạng

### Bộ giao thức TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) là bộ giao thức truyền thông căn bản của Internet, bộ giao thức này cũng được sử dụng hệ thống mạng riêng (như intranet hay extranet). Bộ giao thức được cấu thành từ hai giao thức riêng là TCP (Giao thức điều khiển giao vận) và IP (Giao thức liên mạng), chúng được phát triển bởi Bob Kahn và Vint Cerf vào năm 1978. Như nhiều bộ giao thức khác, TCP/IP được coi là một tập hợp các tầng, mỗi tầng giải quyết một tập các vấn đề liên quan đến truyền dữ liệu, cung cấp cho các giao thức tầng cấp trên một dịch vụ được định nghĩa dựa trên việc sử dụng dịch vụ của tầng thấp hơn. Hình dưới đây mô tả cấu trúc của TCP/IP:



***Hình 1.2. Cấu trúc của TCP/IP***

TCP/IP có 4 tầng. Tầng Application (Ứng dụng) chứa các giao thức phổ biến, mỗi giao thức lại có chức năng khác nhau như SMTP (chuyển mail), SNMP (quản lý mạng), FTP (chuyển tệp tin) và HTTP (duyệt web), các chương trình sẽ sử dụng các giao thức tùy theo mục đích của chương trình đó. Sau khi xử lý yêu cầu của chương trình, các giao thức của tầng ứng dụng sẽ chuyển yêu cầu xuống tầng Transport (Vận chuyển), tầng này chịu trách nhiệm nhận dữ liệu được gửi từ tầng ứng dụng, chia chúng thành các gói và gửi xuống tầng Internet (Mạng). Đôi khi, trong quá trình tiếp nhận dữ liệu, tầng vận chuyển có thể đưa dữ liệu vào hàng dợi do quá tải, tầng này cũng có thể kiểm tra tính toàn vẹn của dữ liệu. Khi nhận được gói tin từ tầng vận chuyển, tầng mạng sẽ cung cấp địa chỉ ảo cho gói tin, địa chỉ ảo này được gọi là địa chỉ IP – những IP này chứa địa chỉ máy gửi và máy nhận gói tin. Sau đó, gói tin sẽ được chuyển xuống tầng Network Interface (Giao diện), tầng này có nhiệm vụ nhận gói tin từ tầng mạng và gửi chúng đến địa chỉ được định sẵn hoặc ngược lại (*Gabriel Torres,2012. How TCP/IP Protocol Works-Part 1*).

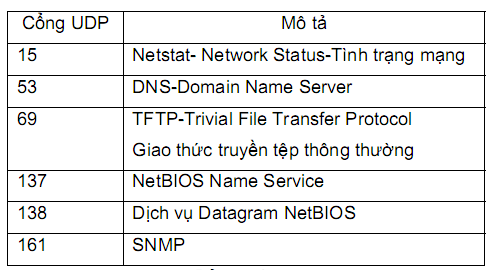
### Giao thức UDP

UDP là giao thức thay thế của TCP/IP, tên đầy đủ là User Datagram Protocol. Không giống như TCP/IP, UDP không chia thành các gói tin khi truyền tải, điều này khiến việc truyền dữ liệu trở lên nhanh hơn nhưng lại khó kiểm soát được lỗi. “Khi sử dụng UDP, gói tin chỉ tới bên nhận, bên gửi sẽ không chờ đợi để đảm bảo bên nhận đã nhận được gói tin hay không mà tiếp tục gửi các gói tiếp theo và nếu bên nhận nhận được gói tin xấu, thì họ không thể yêu cầu bên gửi gửi lại gói tin đó nữa. Do bản chất không trạng thái nên UDP trở nên hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu. Những ứng dụng phổ biến sử dụng UDP như các chương trình phát sóng trực tiếp hay trò chơi trực tuyến.



***Hình 1.3. Phát trực tiếp sử dụng giao thức UDP***

Để sử dụng được UDP, ứng dụng sẽ phải cấp một địa chỉ IP và một cổng UDP đích, cổng này có nhiệm vụ cung cấp vị trí cần gửi gói tin. Hình dưới đây mô tả một số cổng UDP thông dụng:



***Hình 1.4. Một số cổng UDP phổ biến***

### So sánh giữa giao thức UDP và TCP

* Giống nhau: Cả UDP và TCP đều có chức năng kết nối các máy với nhau và được sử dụng để gửi các bit dữ liệu – hay các gói tin trên internet.
* Khác nhau: Các header của TCP và UDP khác nhau ở kích thước (20 và 8 bytes) nguyên nhân là do TCP phải hỗ trợ nhiều chức năng hơn (như khả năng phục lỗi). UDP dùng ít byte hơn cho phần header và yêu cầu xử lý từ host ít hơn.

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| Dùng cho mạng WAN | Dùng cho mạng LAN |
| Không cho phép mất gói tin | Cho phép mất dữ liệu |
| Đảm bảo việc truyền dữ liệu | Không đảm bảo |
| Tốc độ truyền thấp hơn UDP | Tốc độ truyền cao |

### Giao thức ICMP

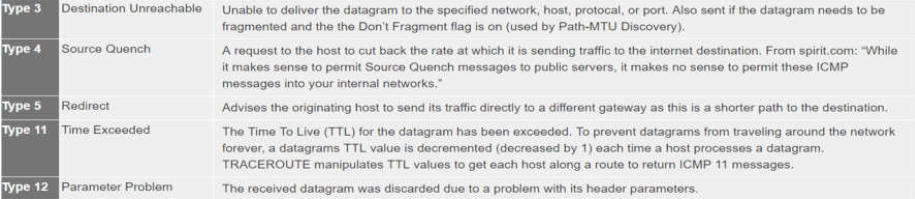
Giao thức ICMP (Internet Control Message Protocol) là giao thứ của gói Internet

Protocol. Giao thức này được các thiết bị mạng như router sử dụng để gửi đi các thông báo lỗi nhằm chỉ ra dịch vụ hay một địa chỉ host có tồn tại hay không.

“ICMP không phải là một giao thức vận chuyển gửi dữ liệu giữa các hệ thống và cũng không được người dùng sử dụng thường xuyên ngoài quản trị viên – là người chuyên giám sát hệ thống mạng, cần kiểm tra hay xử lý các sự cố về mạng, thì các giao thức ICMP cung cấp một số công cụ hữu ích như ping hoặc traceroute để hỗ trợ việc kiểm tra.

Giao thức ICMP có 2 dạng thông báo là thông báo lỗi và thông báo truy vấn.

Cụ thể:



***Hình 1.5. ICMP dạng báo lỗi***



***Hình 1.6. ICMP dạng truy vấn***

Ngoài ra, giao thức ICMP đã từng được sử dụng để thực hiện tấn công từ chối dịch vụ bằng cách gửi gói tin có kích cỡ lớn hơn số lượng bytes cho phép trong giao thức IP.

## Các kỹ thuật và giao thức giám sát cơ bản

Để đảm bảo việc giám sát mạng, máy chủ hay các hệ thống thành công, cần có 3 yếu tố sau:

* Dữ liệu (thông tin) từ nhiều thành phần khác nhau trong mạng. Dữ liệu chứa thông tin về trạng thái, hiệu suất của các thành phần được giám sát.
* Những ứng dụng hoặc phần mềm giám sát phải có chức năng thu thập, xử lý và trình dữ liệu theo cơ cấu thân thiện với người dùng. Phần mềm nên có chế độ cảnh báo cho người dùng biết về các vấn đề sắp xảy ra dựa trên các ngưỡng.
* Phải có giao thức hoặc các cách chuyển giao thông tin giữa các thành phần giám sát và phầm mềm giám sát.

Những kỹ thuật giám sát này được dùng để thu thập thông tin giám sát trên mạng. Có 4 kỹ thuật căn bản là:

* *Ping*: Đây là công cụ quản trị được tích hợp sẵn trong hệ điều hành và được sử dụng để kiểm tra tính sẵn có của các host trên mạng. Kết quả sau khi ping có thể giúp xác định các host trong mạng có đang hoạt động hay không, hơn nữa, kỹ thuật này có thể đo khoảng thời gian dịch chuyển các gói tin và thông báo gói tin bị mất khi kết nối với host.
* *Giao thức quản lý mạng đơn giản (Simple Network Management Protocol):* Là giao thức chuyển đổi thông tin giữa các host trên mạng – bao gồm cả phần mềm giám sát mạng. Giao thức này được sử dụng rộng rãi nhằm quản lý và giám sát các thành phần mạng như:
* Các thiết bị mạng: Tất cả các thiết bị mạng có hỗ trợ giao thức SNMP
* Các agent: Là một chương trình có trong các thiết bị được giám sát. Agent có khả năng truy cập vào trong MIB – tạm gọi là cơ sở quản lý thông tin của thiết bị, cho phép NMS – hệ thống quản trị mạng đọc và viết trong MIB.
* Hệ thống quản trị mạng (NMS): Là một ứng dụng trên hệ thống giúp giám sát, điều khiển các thiết bị qua các agent sử dụng lệnh SNMP.
* *Syslog (System Log):* Là nơi lưu trữ số lần đăng nhập hệ thống, cho phép các thiết bị gửi các thông báo sự kiện trong mạng. Thông tin từ những thông báo này có thể được dùng để quản lý hệ thống. Syslog có thể hỗ trợ đa thiết bị từ máy in, router hay tường lửa.
* *Sử dụng các tập lệnh có sẵn*: Trong hệ thống mạng không sử dụng NMS để giám sát hoặc NMS không hỗ trợ một chức năng cụ thể, quản trị viên có thể sử dụng các tập lệnh có sẵn. Những tập lệnh này sử dụng các câu lệnh căn bản như ping, netstat, snmpwalk, …, chúng được hỗ trợ bởi hầu hết các thành phần mạng nhằm thực hiện hành động như thu thập dữ liệu từ các thành phần mạng, tạo các thay đổi trong cấu hình thiết bị hay thực hiện các nhiệm vụ theo kế hoạch.

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

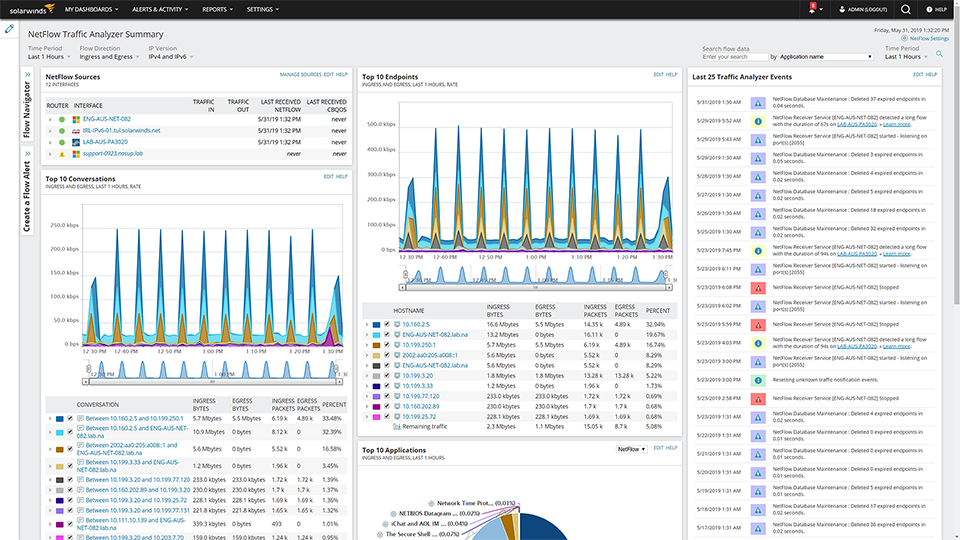
### Mô hình FCAPS (Fault Configuration Accounting Performance Security)

Một trong các quy tắc khi thiết kế hệ thống giám sát là tuân theo mô hình FCAPS. “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 (Configuration Management), quản lý kế toán (Accounting Management), quản lý hiệu năng (Performance Management) và quản lý bảo mật (Security Management).

* *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 chủ động quản trị và giám sát mạng.
* *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, … 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.

### Báo cáo và cảnh báo

Công việc của giám sát mạng là thu thập 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.



***Hình 1.7. Minh họa về bản báo cáo 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 gây sụp đổ toàn hệ thống.

### Một số thuật ngữ liên quan đến cảnh báo

* *Triggers*: Tên tiếng việt là sự kích hoạt. Sự kích hoạt được tạo ra khi có một sự kiện xảy ra – có thể là việc thay đổi các nút mạng hay giá trị trên các nút, độ lệch giá trị trung bình của tham số, và hơn thế nữa.
* *Ngưỡng, đếm lặp và thời gian trễ*: Phần lớn các cảnh báo được tạo ra dựa trên ngưỡng. Khi các giá trị cơ sở của tham số vượt quá mức cho phép, xung đột ngưỡng xảy ra và có thể thiết lập kích hoạt cảnh báo. Chế độ cảnh báo cũng có thể được thiết lập khi các ngưỡng xung đột dựa trên số lần đếm lặp và thời gian trễ.
* *Thiết lập lại*: Chế độ cảnh báo được tạo ra nhờ xung đột ngưỡng sẽ thiết lập lại khi giá trị tham số trở về giá trị ban đầu.
* *Ngăn chặn và chống trùng lặp*: Một số các xung đột ngưỡng được chấp nhận ngay cả khi chúng vượt mức giá trị. Trong trường hợp đó, các cảnh báo được chặn lại, để làm điều này, hệ thống giám sát có hỗ trợ chống trùng lặp, thậm chí hợp nhất các thông báo dựa trên các sự kiện gây ra sự kích hoạt.

### Tích hợp lưu trữ dữ liệu

Hệ thống giám sát thu thập 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 lớn 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 vậy 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.

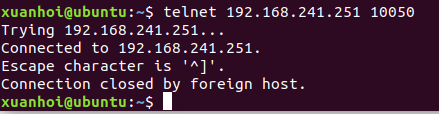
## Các vấn đề trong giám sát mạng

### Giám sát khả dụng (Availability Monitoring)

Kiểu giám sát này định nghĩa cách thức giám sát của toàn bộ tài nguyên trong cơ sở hạ tầng công nghệ thông tin, đảm bảo tính sẵn có để phục vụ cho các yêu cầu của tổ chức hoặc người dùng. Mạng và các dịch vụ cung cấp trong mạng cần tính sẵn có trong suốt thời gian nhằm đảm bảo tiến độ công việc. Việc giám sát liên tục tài nguyên và dịch vụ nhằm đảm bảo các nút mạng hay dịch vụ không bị sập, đảm bảo tính sẵn có khi gặp các yêu cầu.

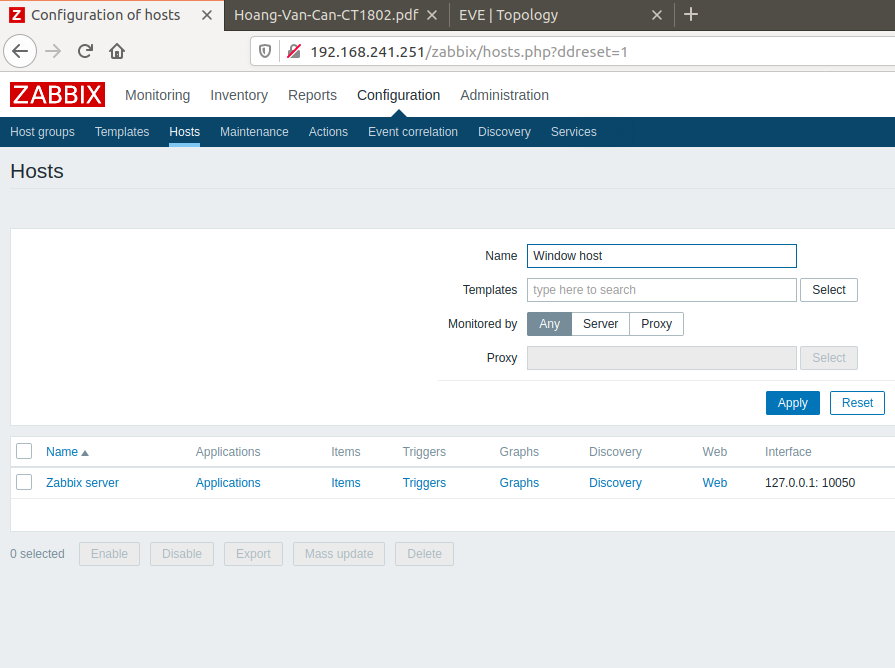
Các kỹ thuật thường dùng trong giám sát sẵn có là:

* *Ping*
* *Telnet*: Dùng để kiểm tra tính sẵn có của thiết bị trong mạng (kiểm tra xem 2 bên có kết nối được với nhau không)



***Hình 1.8. Lệnh telnet trên ubuntu***

* *SNMP*: Dùng để đo trạng thái hiện tại của thiết bị



***Hình 1.9. Dùng SNMP để giám sát trên Zabbix***

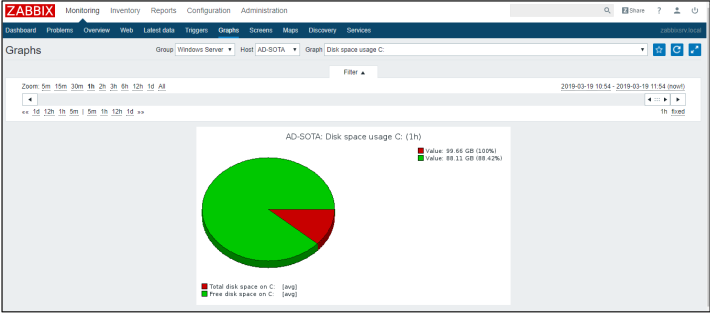
* *WMI (Windows Management Instrumentation):* Tạm dịch là quản lý thiết bị đo trên hệ thống Windows. Thường dùng để kiểm tra các dịch vụ trên Windows.
* *IPSLA (Internet Protocol Service Level Agreement):* Là tính năng của hệ thống Cisco. Có nhiệm vụ kiểm tra tính sẵn có của các liên kết WAN và dung lượng khi phục vụ một dịch vụ nhất định.

### Giám sát giao diện (Interface Monitoring)

Có rất nhiều loại giao diện khác nhau trong mạng như Fast Ethernet và Gigabit Ethernet. Giao diện trên thiết bị là cổng vào và là cổng ra của gói dữ liệu cung cấp dịch vụ cho tổ chức. Việc theo dõi giao diện là việc theo dõi các lỗi, các gói dữ liệu bị mất hay hạn mức sử dụng trên thiết bị, thông tin trên giao diện sẽ giúp tìm ra các vấn đề về mạng.

### Giám sát mức độ sử dụng ổ đĩa (Disk Monitoring)

Dữ liệu hay thông tin là một trong những nguồn tài nguyên quan trọng nhất của tổ chức. Các tổ chức cần dữ liệu cho công việc của họ, vì thế, nó được lưu lại trong ổ đĩa đề sau này sử dụng. Trong doanh nghiệp, dữ liệu được thu thập, lưu trữ trong mảng lưu trữ có nhiều ổ đĩa, bất kỳ vấn đề nào phát sinh trên đĩa hay trên mảng lưu trữ dữ liệu đều có thể gây ra những hậu quả nghiêm trọng đối với công việc kinh doanh.



***Hình 1.10. Lưu lượng ổ đĩa trên AD-SOTA***

Việc giám sát này cho phép quản trị viên lập kế hoạch cho việc nâng cấp hệ thống, nhất là dung lượng, phát hiện các vấn đề lưu trữ liên quan và giảm thời gian chết nếu có sự cố xảy ra.

### Giám sát phần cứng

Có rất nhiều thiết bị phần cứng trong mạng. Cấu trúc phần cứng là xương sống của toàn bộ cơ sở hạ tầng công nghệ thông tin. Nếu một ổ cứng vật lý bị hỏng sẽ dẫn đến việc mạng truyền sẽ chậm và để đảm bảo điều này không xảy ra, việc theo dõi độ ổn định và hiệu suất của thiết bị phần cứng trong mạng là điều rất quan trọng.

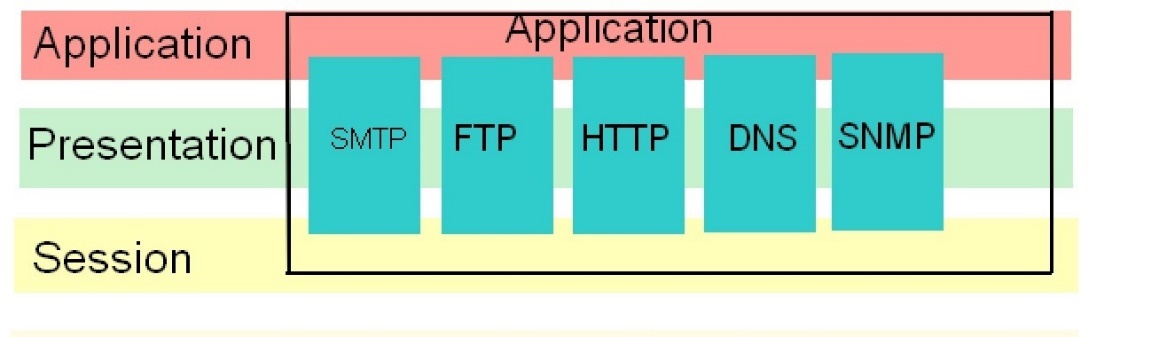
Có rất nhiều số liệu cần được giám sát trong phần cứng. Dưới đây là một số cái quan trọng:

* *CPU*: Các công việc của thiết bị thường do CPU xử lý. Nếu giá trị sử dụng CPU chạm mức giới hạn, hiệu suất của thiết bị có thể gặp ảnh hưởng.
* *Nhiệt độ*: Khi các công việc đang được thực hiện, mức sử dụng của CPU cũng gia tăng, điều này sẽ kéo nhiệt độ của thiết bị lên đến mức độ nào đó, có thể làm hỏng thiết bị cùng với đó là cả hệ thống mạng.
* *Tốc độ quạt*: Kiểm soát tốc độ quạt giúp đảm bảo quạt hoạt động ổn định và làm mát thiết bị. Giữ nhiệt độ luôn ở mức chấp nhận được.
* *Nguồn cấp điện:* Một nguồn cấp điện bị lỗi có thể khiến thiết bị không hoạt động và dẫn tới việc sập mạng.

Việc giám sát với cảnh báo ngưỡng này sẽ giúp quản trị viên sớm tìm ra các vấn đề tiềm ẩn trong hệ thống, từ đó, đưa ra được cách khắc phục kịp thời, đảm bảo đường mạng luôn thông suốt.

## Tổng quan về giao thức SNMP

Như đã giới thiệu ở phần đầu, giao thức SNMP là một giao thức chuẩn trong giám sát các thiết bị mạng và phần mềm, thuộc tầng thứ 7 trong mô hình OSI và là một phần của bộ giao thức TCP/IP.



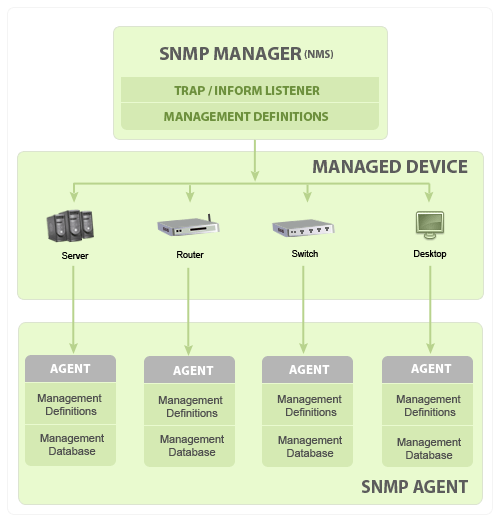
***Hình 1.11. Vị trí SNMP trong mô hình OSI***

### Các thành phần cơ bản trong SNMP

SNMP bao gồm 4 thành phần cơ bản sau:

* *Hệ quản lý SNMP*: “Hệ thống quản lý là một thực thể riêng biệt có nhiệm vụ giao tiếp với các SNMP agent trên các thiết bị mạng. Thường dùng cho máy tính chạy một hoặc nhiều hệ thống quản trị mạng”. Các chức năng chính của hệ quản lý SNMP là:
* Truy vấn các agent
* Tiếp nhận phản hồi từ phía các agent
* Đặt các biến trong agent
* Nhận biết các sự kiện bất đồng bộ từ phía các agent
* *Quản lý các thiết bị*: Việc quản lý thiết bị hay các thành phần mạng yêu cầu một số hình thức giám sát và quản lý.
* *SNMP agent*: Đây là chương trình hỗ trợ bên trong các thiết bị mạng. Các chức năng chính của SNMP agent là:
* Thu thập thông tin quản lý về môi trường nội bộ
* Lưu trữ và lấy lại dữ liệu trong MIB
* Báo hiệu các sự kiện cho quản lý
* Có thể hoạt động như 1 proxy cho các nút mạng không sử dụng SNMP

Dưới đây là sơ đồ truyền thông cơ bản trong SNMP:



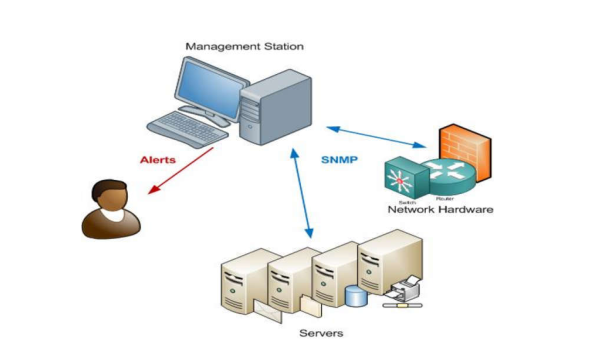
***Hình 1.12. Sơ đồ truyền thông trong SNMP***

* *Cơ sở quản lý thông tin (MIB):* Mỗi một SNMP agent đều chứa đựng thông tin mô tả thông số của thiết bị được giám sát. Hệ quản lý SNMP sử dụng MIB để yêu cầu các thông tin cụ thể, cùng với biên dịch những thông tin cần thiết cho phía NMS từ các agent. Thông thường, các MIB lưu trữ một bộ thống kê tiêu chuẩn cùng các giá trị điều khiển định nghĩa cho các nút phần cứng trên mạng. Nói cách khác, các tập tin MIB là một bộ câu hỏi mà hệ quản lý SNMP có thể yêu cầu các agent thi hành, các agent sẽ theo đó mà thu thập và lưu trữ dữ liệu.

### Chức năng của giao thức SNMP

Dưới đây là một số chức năng của giao thức:

* Cung cấp khả năng đọc/viết (đổi mật khẩu hoặc địa chỉ IP)
* Thu thập thông tin về số lượng băng thông được dùng
* Thu thập các báo cáo lỗi
* Thông báo lỗi qua hệ thống gmail
* Giám sát mức sử dụng của CPU và bộ nhớ. Đưa ra cảnh báo khi ngưỡng vượt giới hạn
* Gửi tin nhắn SMS khi có thiết bị lỗi
* Chủ động thăm dò trạng thái thiết bị
* Các thiết bị SNMP thụ động có thể gửi cảnh báo về máy chủ khi bị gặp sự cố

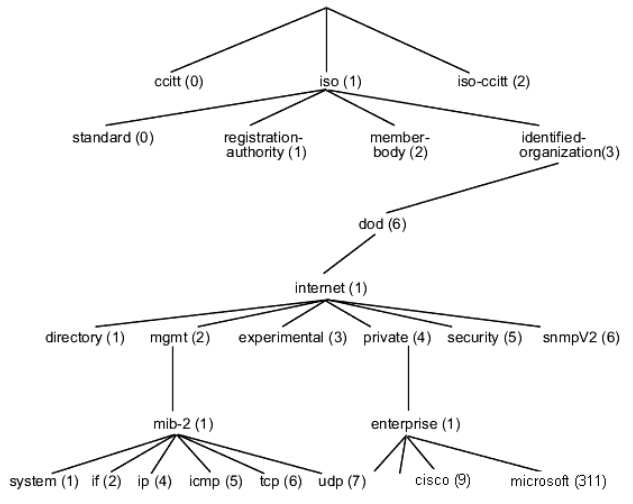


***Hình 1.13. Sơ đồ chức năng cảnh báo của SNMP***

### Sơ lược về Object Identifier (OID)

**“**SNMP hoạt động bằng cách truy vấn đối tượng. Đối tượng đơn giản chỉ là thứ chúng ta có thể lấy thông tin về thiết bị mạng. Ví dụ, trạng thái hiện tại của thiết bị, khi SNMP thực hiện truy vấn sẽ trả về các biến như Up hoặc Down. SNMP xác định đối tượng như một định danh đối tượng hay còn gọi là OID”.

Vậy OID là gì? OID là một chuỗi địa chỉ dùng để xác định thiết bị và trạng thái của thiết bị đó. Chúng được biểu diễn dưới dạng cây phân cấp cấu trúc – giống như cấu trúc thư mục trong máy tính, chỉ khác các đối tượng SNMP là các số.



***Hình 1.14. Sơ đồ phân cấp OID***

Cấp cao nhất sau gốc là iso, có số là 1, tiếp đến là identified - organization, số là 3 và cứ như vậy theo thứ tự. OID luôn được viết theo dạng số thay vì dạng chữ. Ví dụ: số OID của Cisco sẽ là 1.3.6.1.4.1.9.

### Mối liên hệ giữa MIB và SNMP

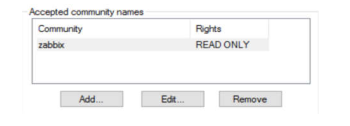
MIB giống như máy phiên dịch có nhiệm vụ giúp hệ quản lý hiểu được phản hồi SNMP từ các thiết bị mạng. Hầu hết các thiết bị SNMP đều hỗ trợ các đối tượng tiêu chuẩn có tên là MIB-2. Tuy nhiên, cũng có một số thiết bị giám sát những đối tượng không nằm trong MIB-2 như nhiệt độ hay tốc độ quạt, vì thế, các nhà sản xuất đã cung cấp một file MIB ở bên ngoài nhằm hỗ trợ cho các tính năng bị thiếu. Những file này sau đó được đưa vào NMS để thông báo với phần mềm rằng đối tượng SNMP nào có thể được truy vấn và hiển thị kết quả như thế nào. Bản thân các file MIB rất khó để đọc một cách thông thường, chúng thường được sử dụng để nhập hay biên dịch bởi hệ quản lý.



***Hình 1.15. File MIB của Cisco***

### Khái niệm về chuỗi community

Là một trong những khái niệm quan trọng khác của SNMP. “Giống như mật khẩu, chuỗi community được dùng để xác thực quyền truy cập của người dùng vào SNMP agent trên thiết bị. Chuỗi community có thể được cấu hình với chế độ read-only (RO) hoặc read-write (RW). Chế độ RO chỉ cho phép thông tin từ phía agent, chế độ RW cho phép người dùng cấu hình lại thuộc tính của thiết bị.



***Hình 1.16. Chuỗi community trong SNMP***

### Các thuật ngữ và cổng sử dụng trong SNMP

Sự đơn giản trong trao đổi thông tin khiến cho SNMP được sử dụng rộng rãi. Dưới đây là một số thuật ngữ trong SNMP:

* *GET*: Được yêu cầu từ phía quản trị viên đến các thiết bị quản lý. Có nhiệm vụ lấy các giá trị từ thiết bị.
* *GET NEXT*: Có chức năng tương tự như GET. Điểm khác biệt nhỏ là GET NEXT lấy các giá trị OID (Object Identifier – Định danh đối tượng) kế trong cây MIB.
* *GET BULK:* Sử dụng để lấy một lượng dữ liệu trong bảng MIB.
* *SET*: Được quản lý dùng để chỉnh sửa hoặc gán giá trị cho các thiết bị được quản lý.
* *TRAPS*: Có thể tạo ra tín hiệu báo về hệ quản lý SNMP khi có sự cố xảy ra.
* *INFORM*: Gần giống như TRAPS, nhưng INFORM cần có xác nhận từ phía hệ quản lý trong việc nhận thông điệp.
* *RESPONSE*: Đưa các giá trị đến trực tiếp cho hệ quản lý.
* *POLLING:* Cơ chế này giúp kiểm tra trạng thái của hệ thống hoặc thiết bị.

SNMP sử dụng 2 cổng UDP (User Datagram Protocol) làm giao thức vận chuyển:

* *UDP 161*: Sử dụng khi bên quản trị giao tiếp với các agent.
* *UDP 162:* Sử dụng khi các agent gửi TRAPS không được yêu cầu tới hệ quản trị.

### Các phiên bản SNMP

Có 3 phiên bản của SNMP là SNMPv1, SNMPv2 và SNMPv3. Tuy nhiên, phiên bản 1 và 2 là hai phiên bản được sử dụng nhiều nhất, SNMPv3 gần đây đã bắt kịp tiến độ để trở nên bảo mật hơn so với hai phiên bản trước.

* *SNMPv1:* Là phiên bản đầu tiên của giao thức này, chúng được định nghĩa trong RFCs (Request for Comments) 1155, 1156 (thay thế bằng 1213 trong MIB-2) và 1157. Vì là phiên bản đời đầu nên tính bảo mật rất kém.
* *SNMPvs2:* Là giao thức cải tiến của SNMPv1 trong các gói giao thức, ánh xạ vận chuyển, các thành phần kiến trúc MIB. Chúng được định nghĩa trong RFC 1901, 1905, 1906 và 2578.
* *SNMPv3:* Là phiên bản bảo mật của SNMP. Phiên bản này tạo thuận tiện cho việc cấu hình từ xa, được định nghĩa trong RFC 1905, 1906, 3411, 3414 và 3415.

### Giám sát hệ điều hành Windows bằng giao thức SNMP

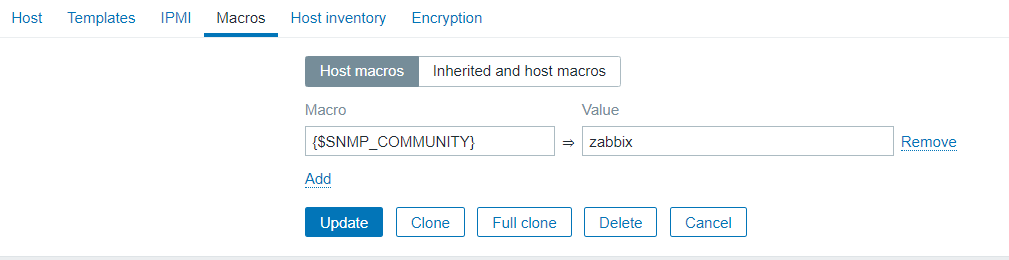
Dưới đây là cách thức hoạt động của giao thức SNMP trong việc giám sát Win10.

Trước hết, phía Zabbix ta chọn “Add host” và điền tên như hình 1.19. Qua mục “Templates”, chọn Template OS Windows như hình 1.17.



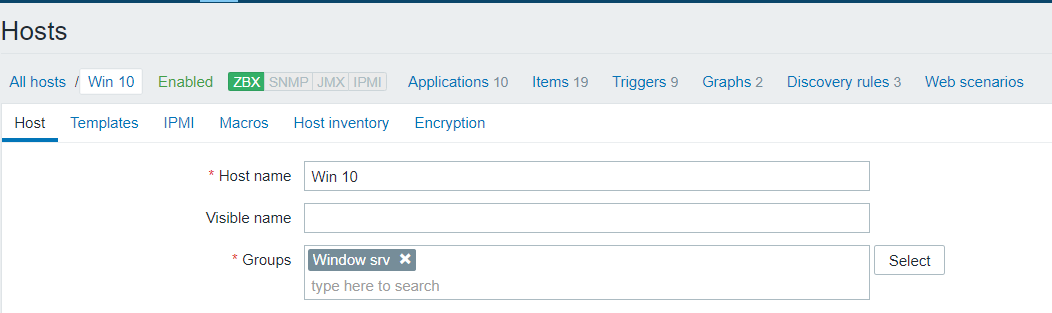
***Hình 1.17. Thêm template cho hệ Windows***

Tiếp theo, chuyển sang tab Macros và điền như hình 1.18



***Hình 1.18. Đặt tên biến trong Macro***

Sau đó, nhấn “Add” để thêm host vừa tạo. Phải mất một lúc, Zabbix mới nhận kết quả.



***Hình 1.19. Zabbix giám sát Win10 qua SNMP***

Ngoài ra, có thể cấu hình cho Zabbix giám sát chính nó bằng SNMP



***Hình 1.20. Zabbix tự giám sát qua SNMP***

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

### Các giải pháp giám sát mạng

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

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

Mô hình của giải pháp quản lý và phân tích sự kiện an ninh gồm 3 thành phần chính:

* 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 nhật ký từ các nguồn thiết bị, ứng dụng.
* Kiểm soát băng thông và không gian lưu trữ thông qua khả năng lưu giữ 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 và lưu trữ.
* Chuyển toàn bộ các sự kiện đã thu thập về thành phần phân tích và lưu trữ.
* 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. Thành phần có 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 quản trị viên.
* Hỗ trợ kết nối đến các hệ thống lưu trữ dữ liệu.
* Thành phần quản trị mạng tập trung:
* Cung cấp giao diện quản trị mạng tập trung cho toàn bộ hệ thống giám sát an toàn mạng.
* Hỗ trợ sẵn 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.
* 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

### Một số công cụ giám sát mạng phổ biến

Trên thế giới có rất nhiều sản phẩm khác nhau, các sản phẩm thương mại (như SolarWinds, CiscoWorks) đều rất đắt tiền (từ vài ngàn USD đến vài chục ngàn USD tùy theo quy mô sử dụng). Việc đầu tư kinh phí cho những sản phẩm này nằm ngoài khả năng kinh tế của phần lớn các cơ quan, doanh nghiệp. Hơn nữa, sau khi triển khai sử dụng, sẽ phải tốn thêm chi phí bảo trì và nâng cấp phần mềm, điều này sẽ gây bất lợi cho doanh nghiệp, không tùy biến được. Chính vì điều đó mà hiện nay, nhiều doanh nghiệp trên thế giới đã chuyển sang lựa chọn mã nguồn mở như một giải pháp tiết kiệm chi phí, các phần mềm giám sát điển hình như Cacti, Zenoss hay Zabbix đã mang lại lợi ích không nhỏ cho doanh nghiệp trong việc giám sát và bảo mật hệ thống mạng. Tất cả đều có đặc điểm chung là miễn phí về giá và bản quyền sử dụng, chỉ cần một người quản trị thiết lập và cài đặt phần mềm trên máy tính là có thể kiểm soát được hệ thống mạng của công ty hay doanh nghiệp.

# TÌM HIỂU VỀ PHẦN MỀM ZABBIX

## Kiến thức chung về phần mềm Zabbix

### Tổng quan

Zabbix là phần mềm mã nguồn mở miễn phí cho doanh nghiệp, sử dụng để giám sát mạng và các ứng dụng, được viết bởi Alexei Vladishev. Phần mềm được thiết kế với mục đích giám sát và tìm ra trạng thái của các thiết bị mạng, máy chủ và các phần cứng khác. Với Zabbix, việc thu thập các loại dữ liệu khác nhau trên mạng rất dễ dàng, Zabbix cung cấp chương trình giám sát thời gian thực hiệu suất cao, có thể giám sát được khoảng 10 nghìn máy chủ, máy ảo cùng các thiết bị mạng. Bên cạnh việc lưu trữ dữ liệu, các tính năng trực quan (như biểu đồ, bản đồ, tổng quát) cũng sẵn có, tiện lợi cho việc phân tích dữ liệu.

Zabbix cung cấp hiệu suất làm việc mạnh mẽ trong việc thu thập dữ liệu. Chúng sử dụng các hệ cơ sở dữ liệu (CSDL) như MySQL, PostgreSQL, SQLite, Oracle hay IBM DB2 để lưu trữ dữ liệu.

### Các tính năng của Zabbix

Zabbix có tất cả 6 tính năng. Mỗi tính năng lại hỗ trợ các phần khác nhau trong hệ thống. Cụ thể:

* *Giám sát mọi thứ:* Với Zabbix, giám sát viên có thể dễ dàng giám sát các máy chủ, các thiết bị mạng, thu thập các số liệu thống kê và hiệu suất dữ liệu. Ngoài ra, tính năng hiệu chỉnh trên Zabbix giúp tích hợp phần mềm trên nhiều môi trường khác nhau. Không có giới hạn về ngôn ngữ kịch bản hay ngôn ngữ lập trình được sử dụng.
* *Hỗ trợ cho doanh nghiệp:* Zabbix được thiết kế để hỗ trợ cho các doanh nghiệp nhỏ và lớn 24/7. Có thể dễ dàng thiết lập và bảo trì việc giám sát phân phối với các proxy, tối ưu hóa hiệu suất sử dụng của CPU hay tích hợp 2 chiều dễ dàng với Zabbix API.
* *Chủ động giám sát:* Tính năng này giúp cho doanh nghiệp giảm thiểu chi phí và thời gian, cải thiện chất lượng dịch vụ. Zabbix có thể gửi các thông báo qua email, SMS hay Jabber (trong giao thức XMPP) về vấn đề đang xảy ra trên hệ thống cho quản trị viên, quản lý các vấn đề hiệu quả và tự động cung cấp những thông tin hữu ích để quản trị viên giải quyết sự cố nhanh hơn, đưa hệ thống hoạt động trở lại bình thường.
* *Lập kế hoạch dung lượng:* Với những dữ liệu thu thập từ Zabbix, các doanh nghiệp có thể dễ dàng phân tích và đưa ra các giải pháp thích hợp, ví dụ khi dung lượng ổ đĩa đầy, các giám sát viên sẽ biết được đến lúc nào phải sử dụng một ổ đĩa mới, tránh việc mất mát dữ liệu. Hơn nữa, lập kế hoạch dung lượng sẽ giúp giảm thiểu sự lãng phí tài nguyên vì trong Zabbix, giám sát viên có thể dễ dàng xác định độ dư thừa của CPU, bộ nhớ hoặc băng thông mạng không chỉ ở một thiết bị mà là toàn bộ hệ thống. Với cách làm này, nhân viên giám sát có thể sắp xếp lại các ứng dụng hoặc thiết bị để sử dụng tài nguyên một cách tốt hơn.
* *Là một mã nguồn mở đúng nghĩa:* Zabbix được phát hành dưới giấy phép của GPL (General Public License), hoàn toàn miễn phí, không có giới hạn về thiết bị giám sát và người dùng có thể chỉnh sửa mã nguồn để phù hợp với hệ thống hay phát triển các công cụ tùy chỉnh để tích hợp vào Zabbix.
* *Là giải pháp cho kinh doanh:* Zabbix cung cấp dịch vụ như tư vấn hỗ trợ, phát triển nhằm tạo cho người dùng trải nghiệm tốt hơn với phần mềm. Ngoài ra, nhóm phát triển Zabbix cũng đưa ra các chương trình huấn luyện như “Chứng chỉ chuyên gia Zabbix” và “Zabbix cho môi trường rộng lớn”, mỗi chương trình thiết kế cho những người dùng riêng biệt.

### Các chức năng của Zabbix

Phần mềm Zabbix có rất nhiều chức năng khác nhau. Mỗi chức năng lại có một nhiệm vụ riêng, có tất cả 10 chức năng trên Zabbix:

* *Thu thập dữ liệu:* Zabbix có một chức năng đồ sộ có thể giúp người dùng giám sát các thứ khác ngoài các host.



***Hình 2.1. Phương pháp để Zabbix lấy dữ liệu***

Các phương pháp này cung cấp sự linh hoạt cho quản trị viên trong việc chọn lựa các cách thức phù hợp cho từng trường hợp.

* *Phát hiện sự cố:* Khi các dữ liệu được thu thập, quá trình đánh giá việc này bắt đầu. Khi ngưỡng trigger chạm mức, trigger sẽ chuyển từ trạng thái ‘OK’ sang ‘PROBLEM’ và ngược lại nếu dưới ngưỡng.
* *Hình dung:* Con người hình dung dữ liệu tốt hơn là những con số khô khan, nhất là khi đó là một lượng dữ liệu không nhỏ.
* *Thông báo:* Zabbix không chỉ giúp thu thập, lưu trữ và phân tích thông tin về môi trường giám sát mà còn thông báo cho người chịu trách nhiệm về các sự kiện xảy ra bằng nhiều kênh khác nhau với các tùy chọn. Zabbix cung cấp một quy trình làm việc hoàn chỉnh: gửi thông báo, cho phép ghi nhận các thông tin nhận được, chuyển thông tin cho người khác và xử lý.



***Hình 2.2. Chu trình làm việc của thông báo trong Zabbix***

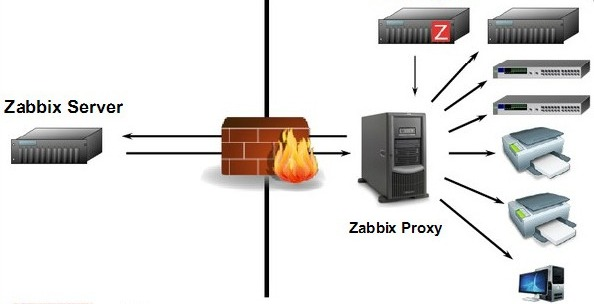
* *Bản mẫu và chức năng nhập/xuất:* Sử dụng bản mẫu là một cách rất hay để duy trì Zabbix một cách dễ dàng hơn. Một tập các chủ đề (các mục, triggers, biểu đồ, …) được gán vào bản mẫu và dùng nó để quản lý hàng ngàn thiết bị khác nhau.



***Hình 2.3. Danh sách các bản mẫu trong Zabbix***

Một bản mẫu có thể liên kết với một số lượng host nhất định. Các mục, triggers và biếu đồ của bản mẫu sẽ được tự động thêm để liên kết với các host đó. Chức năng nhập/xuất trong Zabbix cho phép chuyển đổi cấu hình các chủ đề các chủ thể giữa hệ thống, dữ liệu xuất ra sẽ được đưa về dạng xml.

* *Tự động phát hiện:* Chức năng này có 3 phần chính là phát hiện mạng, phát hiện cấp độ thấp và tự động đăng ký cho các agent đang hoạt động.
* *Giám sát phân tán:* Chức năng này sử dụng zabbix proxy để thi hành nhiệm vụ. Zabbix proxy là phần mềm thu thập thông tin về môi trường được giám sát và gửi lại phía máy chủ Zabbix. Sử dụng Zabbix proxies sẽ rất dễ duy trì môi trường được giám sát, gia tăng hiệu suất cho phía máy chủ Zabbix.



***Hình 2.4. Minh họa cho Zabbix proxy***

* *Bảo mật và xác thực:* Cấp quyền người dùng, quyền truy cập vào host. Sử dụng một số phương thức xác thực như CSDL nội bộ, xác thực bằng giao thức HTTP cơ bản, xác thực LDAP (Lightweight Directory Access Protocol – Giao thức truy cập thư mục nhỏ) và mã hóa các thành phần Zabbix.
* *Quản trị hệ thống:* Giúp hỗ trợ các đợt bảo trì. Quản trị viên có thể cài đặt các đợt bảo trì (hằng ngày, hàng tuần hay hàng tháng) trên Zabbix một cách dễ dàng, bên cạnh đó, chức năng này còn hỗ trợ 2 chế độ bảo trì, cho phép quản trị viên dừng việc thu thập dữ liệu hoặc loại bỏ các thông báo lỗi trong khi vẫn thu thập dữ liệu trong thời gian bảo trì. Ngoài ra, chức năng quản trị cũng hỗ trợ việc kiểm tra thông tin của host, đồng thời đưa ra các câu lệnh tùy chỉnh để quản lý các host này.
* *Zabbix API (Application Programming Interface):* Tạm dịch là giao diện lập trình ứng dụng, cung cấp quyền truy cập cho tất cả các chức năng trong Zabbix. Việc này đã mở ra rất nhiều cơ hội, thậm chí ảnh hưởng lớn tới việc giám sát, cụ thể:
* Có thể tích hợp 2 chiều dễ dàng.
* Có thể dùng chung với phần mềm thứ 3.
* Quản lý cấu hình
* Phục hồi dữ liệu

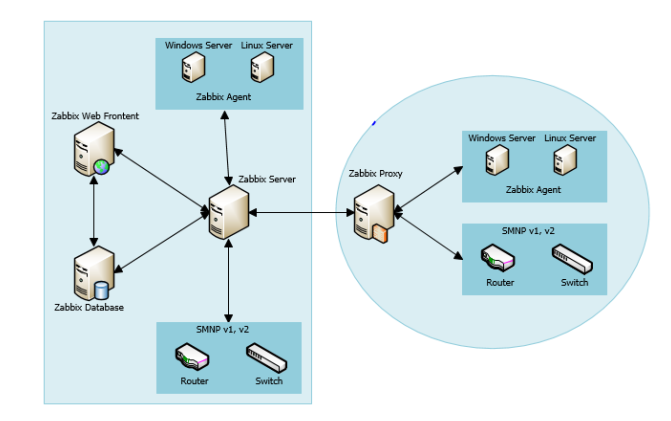
## Ưu nhược điểm của Zabbix so với hệ thống giám sát phổ biến khác

Bất cứ một phần mềm nào cũng có điểm lợi và bất lợi đối với mỗi người sử dụng, Zabbix cũng không nằm ngoài số đó. Bảng dưới đây sẽ cho các nhìn tổng quan về những lợi ích và bất cập của Zabbix so với phầm mềm giám sát thông dụng đó là Nagios.

|  |  |  |
| --- | --- | --- |
|  | Zabbix | Nagios |
| Ưu điểm | * Miễn phí | * Miễn phí |
|  | * Hỗ trợ hầu hết các giao thức (HTTP, SSH, …) | * Hỗ trợ hầu hết các giao thức giống Zabbix |
|  | * Thông báo qua email, chuông hoặc SMS | * Giống Zabbix |
|  | * Giao diện web làm việc, tương tác tốt | * Giám sát nội dung các trang web |
|  | * Hỗ trợ các template, dễ dàng cho việc thêm các host và thiết bị |  |
|  | * Agent cài đặt dễ dàng |  |
|  | * Hỗ trợ báo cáo SLA trong thời gian thực |  |
|  | * Giám sát các trang web toàn diện |  |
|  | * Có thể tùy chỉnh dễ dàng |  |
|  | * Nhạy bén |  |

|  |  |  |
| --- | --- | --- |
| Nhược điểm | * Không phù hợp với hệ thống lớn trên 1000 nút mạng | * Giao diện ít tương tác, chủ yếu để đọc |
|  |  | * Quy trình cài đặt và cấu hình agent phức tạp |
|  |  | * Hỗ trợ báo cáo SLA phải dùng plugin |
|  |  | * Sử dụng addon để thay thế các tính năng bị thiếu |

## Kiến trúc của hệ thống giám sát Zabbix



***Hình 2.5. Kiến trúc của Zabbix***

Kiến trúc của Zabbix bao gồm 4 thành phần cơ bản: Zabbix server, Zabbix proxy, Zabbix agent, Zabbix Web frontend.

* **Zabbix server**

Đây là thành phần trung tâm của phần mềm Zabbix. Server có thể kiểm tra các dịch vụ mạng từ xa (web server và mail server). Agent sẽ báo cáo toàn bộ thông tin và số lượng thống kê cho server. Server sẽ lưu trữ tất cả cấu hình và dữ liệu thống kê.

* **Zabbix proxy**

Proxy là phần tùy chọn của Zabbix. Proxy sẽ thu nhận dữ liệu, lưu trong bộ nhớ đệm và được chuyển đến Zabbix server.

Zabbix proxy là một giải pháp lý tưởng cho một giám sát tập trung của địa điểm từ xa, chi nhánh, mạng lưới không có các quản trị viên địa phương.

Zabbix proxy cũng có thể được sử dụng để phân phối tải của một đơn Zabbix server. Zabbix proxy sẽ giúp giảm tải cho Zabbix server nhờ việc thu thập dữ liệu và chuyển về cho Zabbix server.

Zabbix proxy có thể được dùng để:

* Giám sát các host từ những nơi khác
* Giám sát các host từ những nơi có kết nối không ổn định
* Giảm tải cho Zabbix server khi phải giám sát nhiều thiết bị
* Đơn giản hóa cho việc bảo trì và giám sát

Zabbix Proxy chỉ cần một kết nối TCP đến Zabbix server vì vậy phải cho phép kết nối này khi có tường lửa giữa Zabbix proxy và Zabbix server.

* **Zabbix agent**

Agent là thành phần được cài đặt trên máy chủ, các thiết bị mạng cần giám sát. Agent sẽ thu thập thông tin hoạt động (ổ cứng, bộ nhớ, bộ xử lý số liệu thống kê, …) từ hệ thống mà nó đang chạy và báo cáo dữ liệu này đến Zabbix server để xử lý tiếp. Trong trường hợp lỗi (ổ cứng đầy hoặc một tiến trình chết, …), Zabbix server sẽ gửi cảnh báo cho người quản trị về các sự cố này.

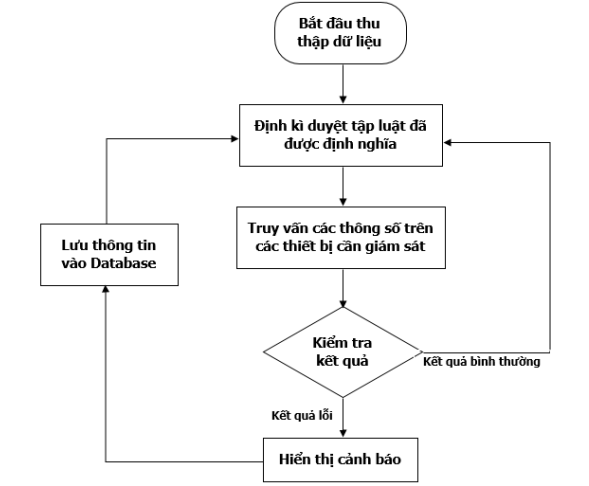
* **Zabbix web frontend**

Là một giao diện web được viết bằng ngôn ngữ lập trình PHP, cho phép người quản trị hệ thống có thể cấu hình, giám sát, xem các dữ liệu thu thập được trên một giao diện web duy nhất.

## Cơ chế hoạt động

Zabbix giám sát các thiết bị qua Zabbix agent hoặc qua giao thức SNMP …

Các agent (thiết bị mạng hay server được cài đặt snmp hay zabbix agent) sẽ gửi các event liên quan đến thiết bị mạng, máy chủ tới Zabbix server, Zabbix server làm nhiệm vụ phân tích số liệu thu thập được và dựa vào các trigger do người quản trị hệ thống thiết lập mà quyết định đưa ra các cảnh báo theo mức độ khác nhau (Critical, Warning hoặc Information…) Hình thức cảnh báo là gửi SMS, email, …



***Hình 2.6. Cơ chế hoạt động của Zabbix***

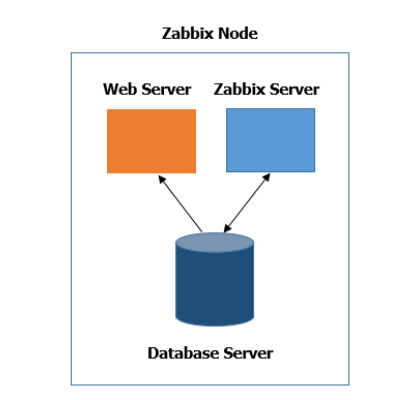
## Các mô hình triển khai hệ thống Zabbix

Nhìn chung, kiến trúc Zabbix cho các hệ thống lớn bao gồm 3 thành phần như sau: Web server, Zabbix server, Database server.

Ngoài ra còn có thêm 2 thành phần nữa bao gồm Zabbix agent và Zabbix proxy. Dựa vào đặc điểm kiến trúc mà Zabbix thông thường được triển khai theo 2 mô hình dưới đây:

* **Mô hình tập trung**

Mô hình cài đặt trên một máy chủ 01 – máy chủ không được khuyến cáo trên các hệ thống giám sát lớn, tuy nhiên đấy là một mô hình cơ bản và phù hợp với doanh nghiệp nhỏ có số lượng thiết bị cần giám sát ít. Một node cài tất cả các thành phần Zabbix server, Zabbix database, Zabbix wed frontend.



Hình 2.7. Mô hình triển khai Zabbix trên một node

Đối với các doanh nghiệp vừa và nhỏ, chúng ta chỉ cần triển khai trên một server vật lý để tiết kiệm chi phí đầu tư phần cứng.

Đối với các doanh nghiệp lớn, cần đảm bảo tính dự phòng của hệ thống thì có thể cài đặt thêm các node dự phòng, share tải và HA (High Available) cho hệ thống.

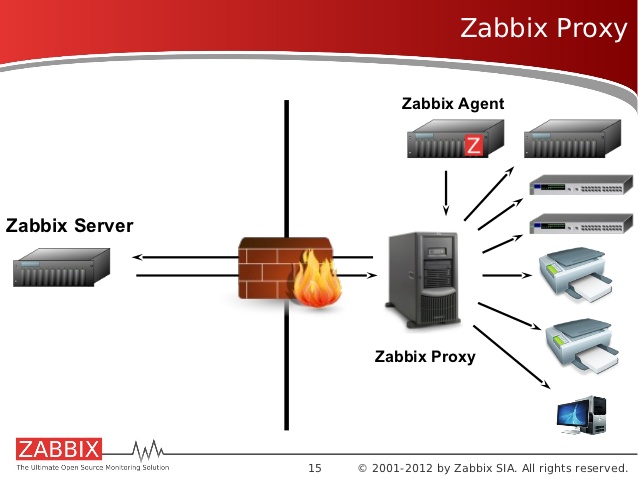
* **Mô hình phân tán**

Zabbix là một ứng dụng giám sát có thể monitor hàng trăm đối tượng trong một mô hình cài đặt single server. Tuy nhiên khi hệ thống mà có đến hàng nghìn máy chủ, thiết bị mạng, với mô hình mạng phức tạp, các máy chủ có thể đặt ở nhiều vị trí địa lý khác nhau thì đây lại là một điểm giới hạn của việc cài đặt single server.

Trong phần lớn trường hợp, trong doanh nghiệp có thể đã có một hệ thống Zabbix đã được cài đặt. Zabbix có ưu điểm về tính linh hoạt, cho phép nâng cấp mô hình cài đặt lên một bước, theo mô hình: proxy-based monitoring (hay mô hình phân tán).

Proxy-based monitoring được triển khai với một Zabbix server và nhiều Zabbix proxies, mỗi proxy có thể ở tại một chi nhánh hoặc một data center. Cấu hình này dễ dàng duy trì và có nhiều ưu điểm triển khai, đặc biệt trong việc giám sát tập trung. Loại kiến thức triển khai này phù hợp với các loại giám sát có mô hình phức tạp.

Kiến trúc giám sát phân tán là mô hình cài đặt phức tạp nhất trong việc triển khai Zabbix. Hình ảnh bên dưới mô tả hệ thống giám sát phân tán kết hợp proxy-based để giám sát.



***Hình 2.8. Mô hình Zabbix phân tán***

## Các thành phần cơ bản trong Zabbix

- *Host:* Các thiết bị mà cần giám sát, có thể là server, máy trạm, thiết bị mang, thiết bị Firewall, UPS, … Tạo một host chính là việc đầu tiên trong cấu hình giám sát Zabbix.

*- Item:* Chính là các đối tượng, dữ liệu cần thu thập trong một host. Có nhiều kiểu item khác nhau, nó phụ thuộc vào các đối tượng giám sát khác nhau.

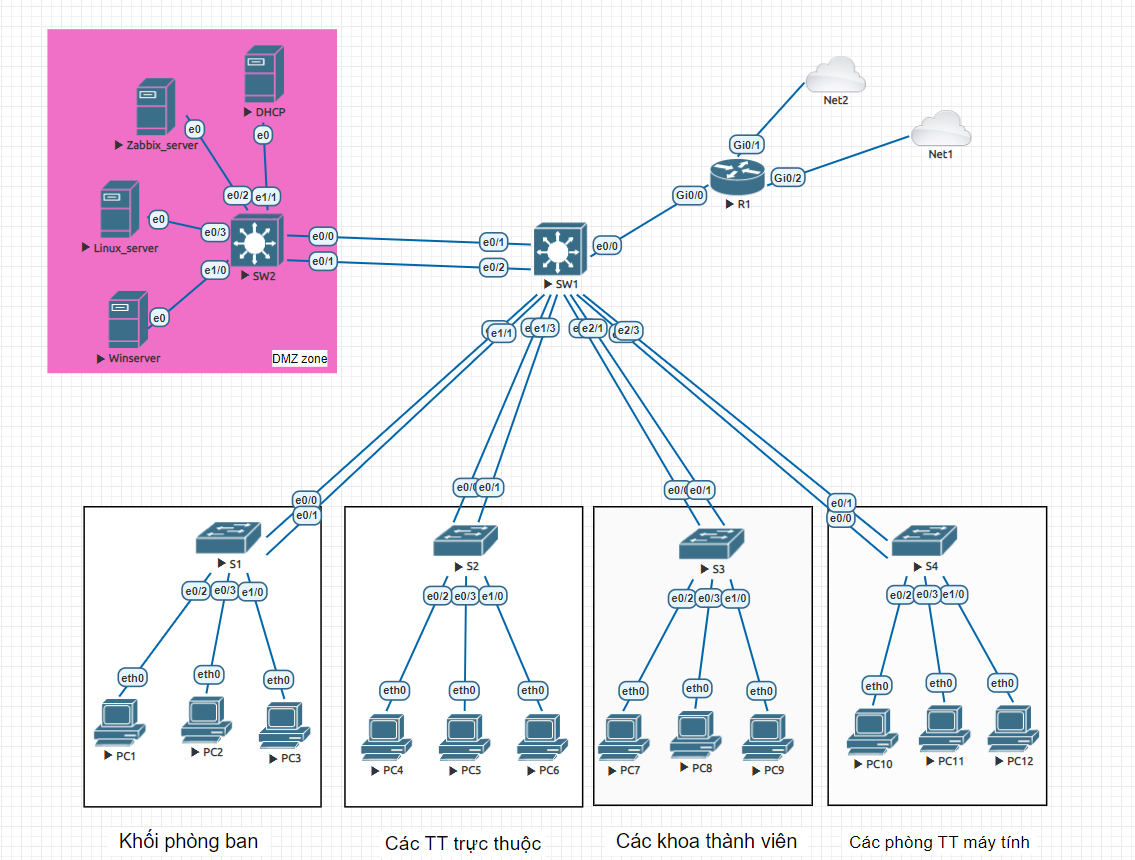
- *Triggers:* Là một điều kiện khi thỏa mãn điều kiện của Triggers mà người lập trình đặt ra thì sẽ thực hiện một hành động nào đó tiếp theo.

- *Template:* Là một mẫu chuẩn, đã được định nghĩa sẵn các item, triggers, graph, screen, … Nó vô cùng thuận tiện khi triển khai giám sát nhiều host có những thành phần cần giám sát giống nhau. Vì vậy, chỉ cần tạo một template là có thể áp dụng nhiều host khác nhau.

# MÔ PHỎNG VÀ ĐÁNH GIÁ

## Sơ đồ mô phỏng

Dưới đây là hình ảnh mô phỏng sơ đồ mạng:



***Hình3.1: Sơ đồ mạng mô phỏng***

Sơ đồ mạng bao gồm:

* Máy Zabbix Server có địa chỉ 10.10.5.20
* Router R1: g0/2 có địa chỉ 192.168.73.120 và g0/1 có địa chỉ 192.168.173.120
* SW1 có địa chỉ 10.10.5.10
* SW2 có địa chỉ 10.10.5.2
* Linux Server có địa chỉ 10.10.5.50
* Win Server có địa chỉ 10.10.5.40

Nhiệm vụ: Máy Zabbix server sẽ giám sát router, switch và các host.

Cụ thể: Với R1, Zabbix sẽ giám sát các cổng g0/1 và g0/2, kiểm tra lưu lượng truyền tải trong từng cổng (tương tự với các switch còn lại). Với các host, Zabbix sẽ giám sát lượng tín hiệu dịch chuyển qua card mạng được dùng cho host, đưa ra biểu đồ thể hiện mức sử dụng dữ liệu trong ổ đĩa ảo hoặc ổ đĩa vật lý.

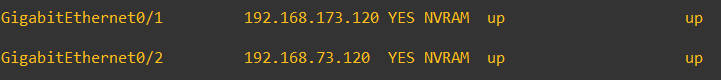
## Kỹ thuật sử dụng

Đồ án này sử dụng phần mềm giả lập mạng EVE-NG (Emulated Virtual Enviroment – Next Generation).



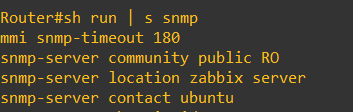
***Hình 3.2. Logo của EVE-NG***

Để giám sát router với switch, trước hết, ta cần gán địa chỉ IP cho các thiết bị. Dưới đây là địa chỉ của R1:



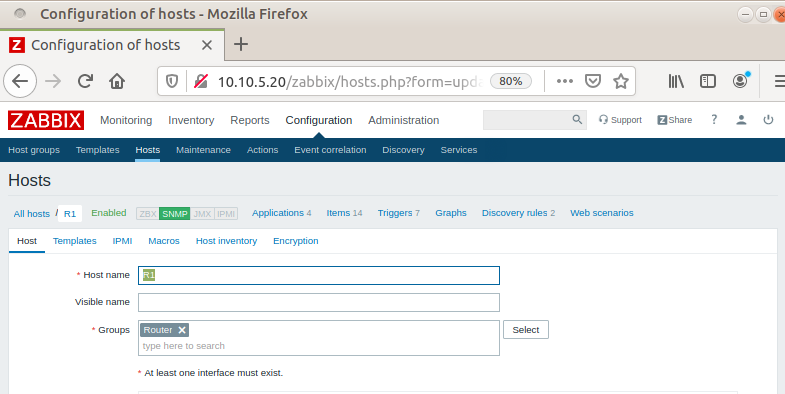
***Hình 3.3. Địa chỉ ip R1***

Sau khi gán địa chỉ cho router, ta tiến hành cấu hình giao thức SNMP với chuỗi community là “public”.



***Hình 3.4. Đặt chuỗi community là “public” cho R1***

Cấu hình giao thức SNMP trên switch tương tự như trên router. Sau khi đặt tên chuỗi community cho R1, ta tiến hành thêm router vào Zabbix server để giám sát.



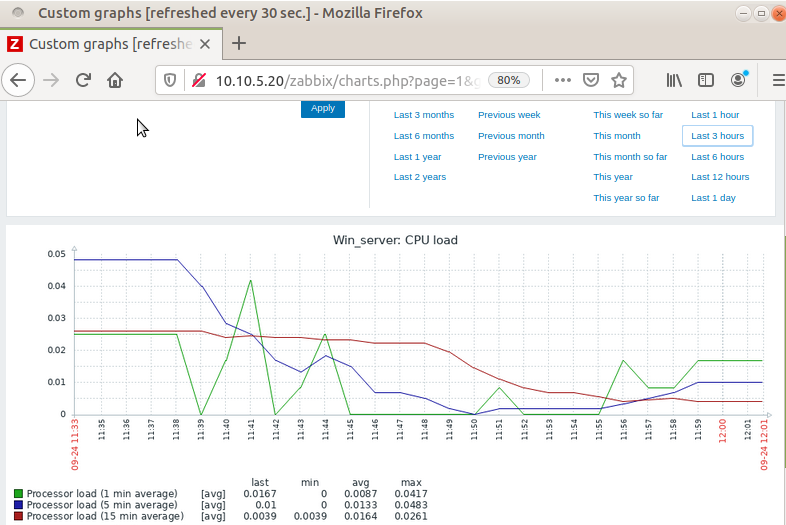
***Hình 3.5. Kết quả giám sát bằng SNMP trên R1***

Để xem chi tiết hơn, ta có thể vào mục ‘Graph’ để xem lưu lượng dịch chuyển trên từng cổng của router.

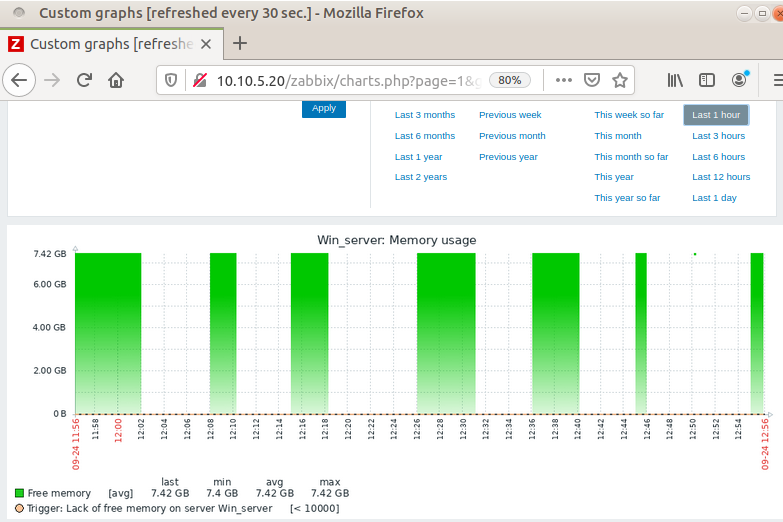
Tiếp theo, ta tiến hành giám sát các host – việc cấu hình các host đã được đề cập ở chương 2. Trong đề tài này sẽ sử dụng 2 nhóm host để giám sát:

* Nhóm Window\_server (Winserver)
* Nhóm Linux servers (Linux\_server)

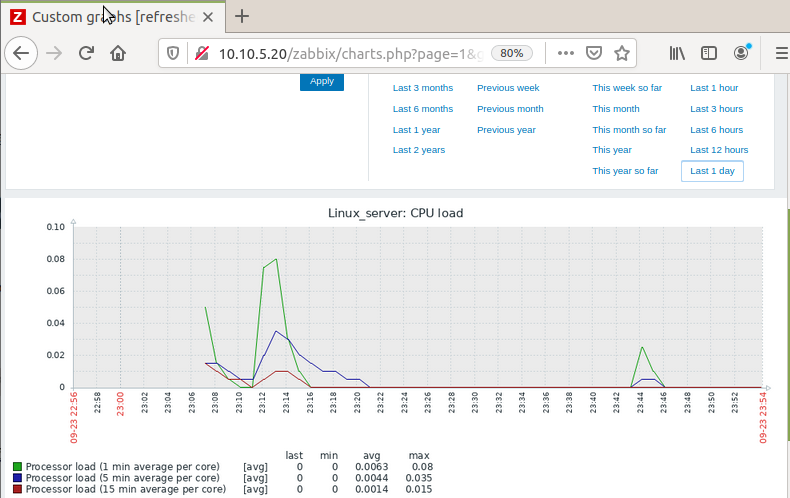
Dưới đây là một số kết quả thu được từ Zabbix



***Hình 3.7: Biểu đồ độ tải CPU trên Win\_server***



***Hình 3.8. Biểu đồ sử dụng RAM của Win\_server***

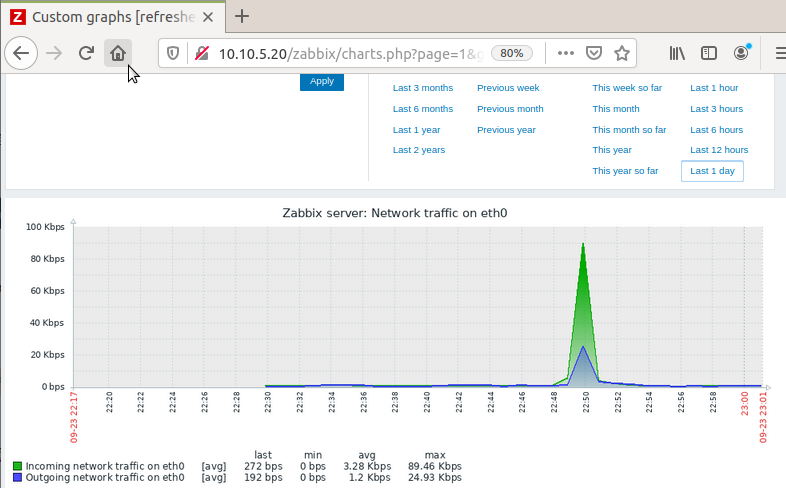


***Hình 3.9: Biểu đồ độ tải CPU trên Linux\_server***

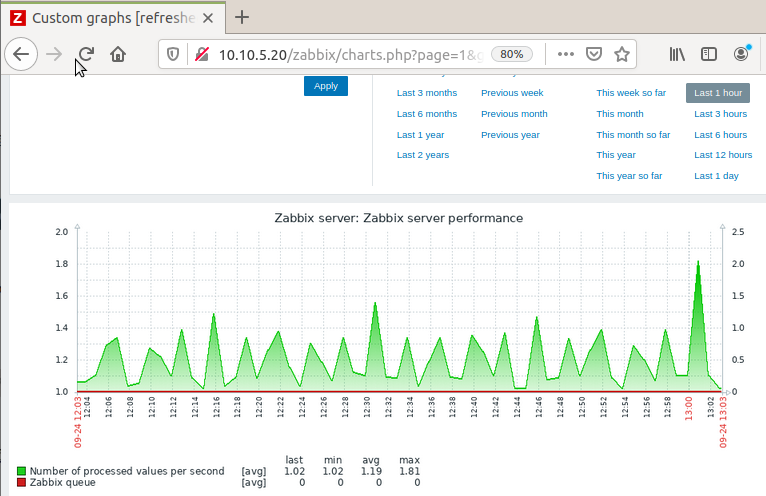


***Hình 3.10. Biểu đồ sử dụng CPU trên Linux\_server***

Ngoài ra, Zabbix có thể tự giám sát chính nó



***Hình 3.11. Lưu lượng truyền tín hiệu trên cổng eth0 của Zabbix server***



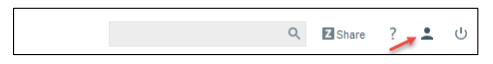
***Hình 3.12. Biểu đồ hiệu năng của Zabbix server***

## Thiết lập cảnh báo

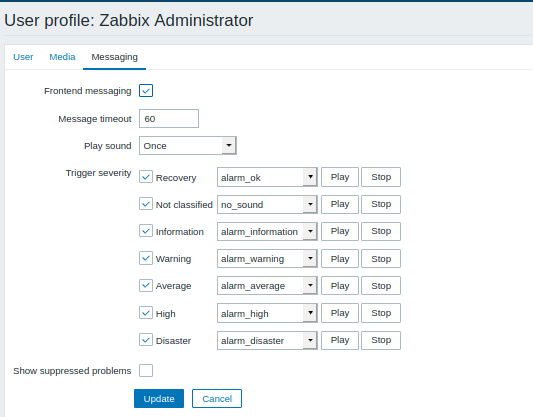
### Cảnh báo tại máy

Hình ảnh và âm thanh trực quan trên web của Zabbix. Hay nói cách khác khi sự cố xảy ra, hệ thống sẽ phát ra tín hiệu cảnh báo như đổ chuông hay hiển thị các hình ảnh cảnh báo. Và nhờ đó, người quản trị viên có thể đưa ra hành động kịp thời cho từng trường hợp cụ thể.

**Bước 1**: Vào Profile của user mà bạn dùng để đăng nhập vào zabbix frontend và sử dụng user đó để nghe thông báo cũng như âm thanh cảnh báo từ Zabbix server.



**Bước 2:** Chọn Messaging −> Tích chọn Frontend messaging



***Hình 3.13. Thiết lập thông tin hiển thị chuông cảnh báo***

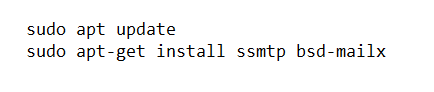
Thiết lập các thông tin cho phù hợp với yêu cầu:

* *Frontend messaging:* Kích hoạt global notification
* *Massage timeout:* Thời gian hiển thị thông báo tin nhắn trigger. Mặc định 60s
* *Play sound:* Chỉ định theo 3 mức sau
* Once: Kêu 1 lần và đầy đủ lượng file âm thanh
* 10 seconds: Âm thanh sẽ lặp đi lặp lại trong vòng 10s
* Message timeout: Âm thanh lặp đi lặp lại cho từng thông báo
* *Trigger severity:* Có thể chỉ định mức trạng thái trigger sẽ được Zabbix thông báo global notification. Giả sử chỉ cần High và Disaster thì chỉ 2 trigger này kích hoạt mới có thông báo âm thanh và khung hiển thị.

### Cảnh báo online

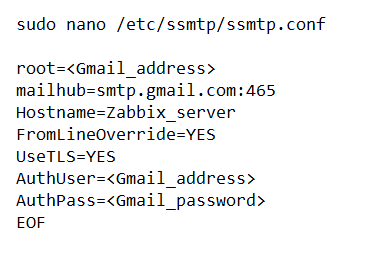
Gửi mail tới mail cá nhân của người quản trị. Do người quản trị không thể ngồi 24/24 trong phòng quản trị được, hay người quản trị đi vắng. Khi đó chúng ta cần thiết lập 1 hệ thống cảnh báo online, từ đó người quản trị có thể truy cập từ xa và quản trị hệ thống được kịp thời, chính xác hay giảm thiểu tối đa thiệt hại khi bị xảy ra sự cố ngoài ý muốn.

**Bước 1**: Cài đặt phần mềm SSMTP

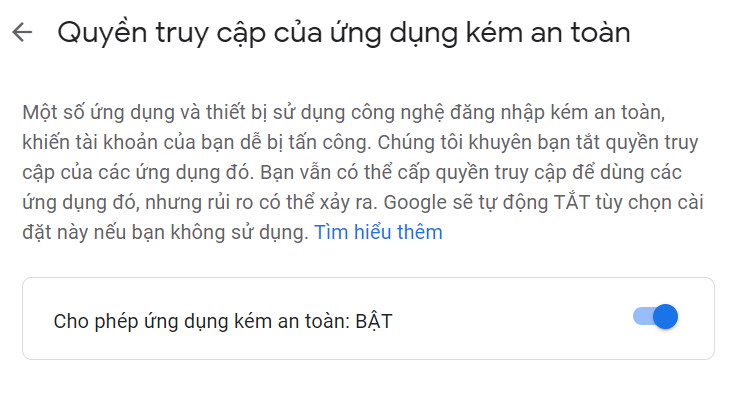


**Bước 2**: Cấu hình các tham số của SSMTP

Lưu ý: Thay đổi các thông số trong dấu <> bằng địa chỉ gmail, mật khẩu, hostname tương ứng.



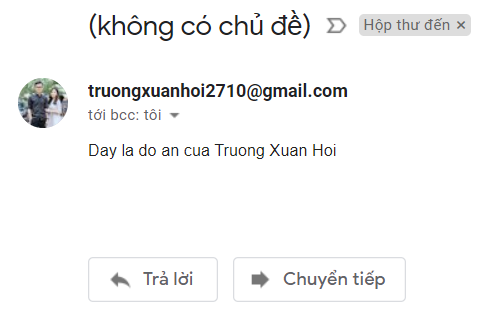
**Bước 3**: Bật tính năng cho phép các truy cập kém an toàn



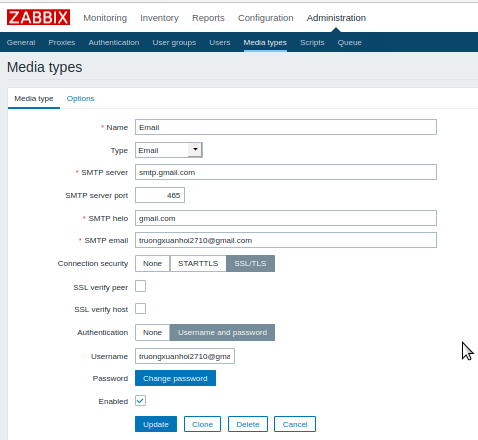
**Bước 4**: Test thử gửi mail bằng dịch vụ SSMTP



Nếu nhận được tin nhắn nghĩa là đã cài đặt thành công



**Bước 5**: Tiến hành cấu hình cho Zabbix server gửi mail cảnh báo vào mail. Đầu tiên, trên giao diện Zabbix, vào mục Adminstration −> Media types −> Email

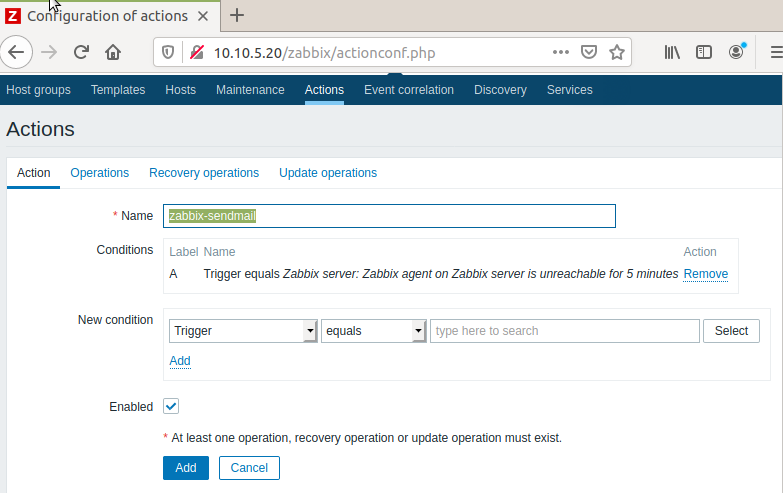


***Hình 3.14. Thiết lập gửi mail cảnh báo***

Hoàn thành các thông tin khai báo email:

* *Name:* Đặt tên dịch vụ là Mail hoặc Alert mail...
* *SMTP server:* Địa chỉ SMTP server
* *SMTP server port:* Port SMTP
* *SMTP email:* Email trong trường hợp này đóng vai trò email gửi lỗi “From address”
* *Connection security:* Giao thức bảo mật tùy chọn theo mail server

**Bước 6**: Để hệ thống thực hiện việc gửi email, cần phải tạo các Triggers. Chọn Configuration −> Actions −> Create action

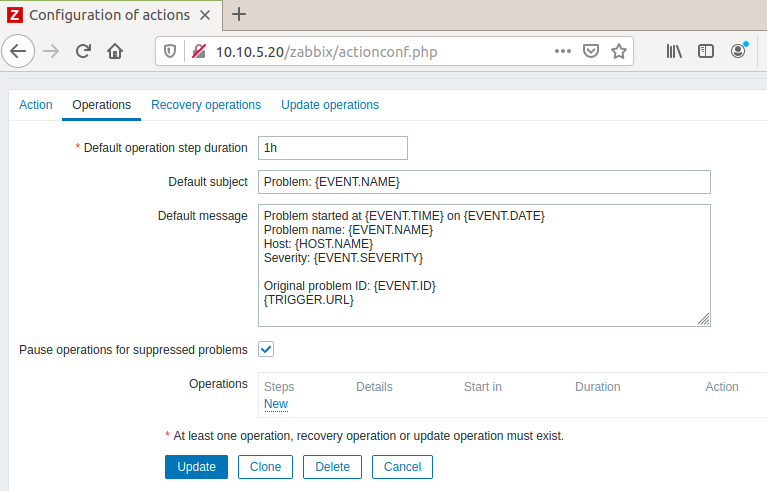


***Hình 3.15. Thiết lập các Triggers để gửi mail thông báo***

Thiết lập theo dõi

* *Name:* Tên dịch vụ
* *New Condition:* Chọn giá trị muốn theo dõi qua mail
* Lựa chọn các điều kiện muốn theo dõi

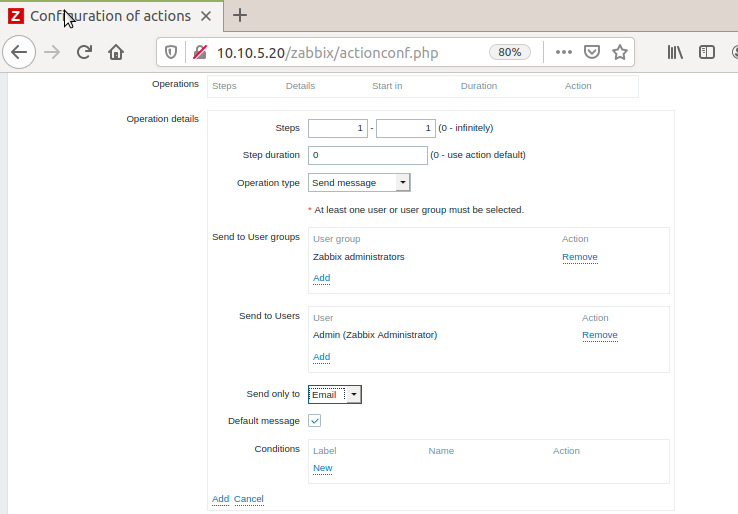
**Bước 7**: Trong tab Operations bao gồm thông tin mà hệ thống sẽ gửi về email, các thông tin này sẽ được chèn vào trong vị trí code. Trong mục Operations chọn New



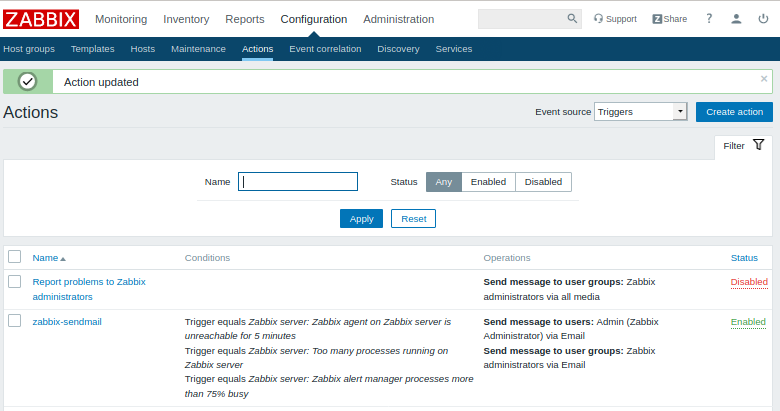
***Hình 3.16. Thiết lập các hoạt động cảnh báo***

Thiết lập các thông tin User Group hoặc nhận thông tin thông báo của hệ thống

* *Send to User groups:* Nhận thông tin thông báo của hệ thống
* *Send to User:* Nhận thông tin thông báo của hệ thống
* *Send only to:* Hình thức gửi

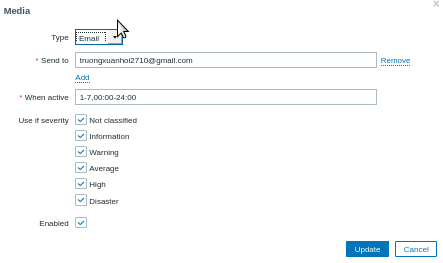


***Hình 3.17. Thiết lập mail nhận thông báo***



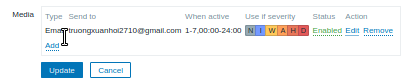
***Hình 3.18. Hoàn thành thiết lập mail cảnh báo qua mail***

**Bước 8**: Vào profile của user −> Media −> nhập địa chỉ email mà ta muốn gửi cảnh báo đến và chọn Add



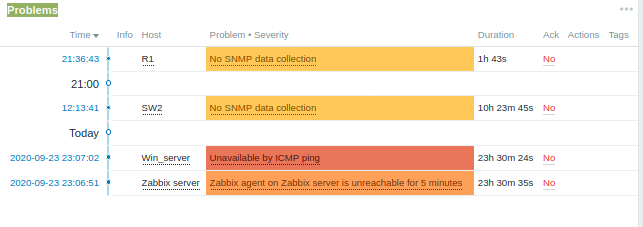
***Hình 3.19. Thiết lập mail nhận thông báo***

Cuối cùng, ta chọn Update để hoàn tất

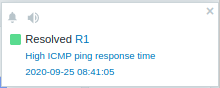


## Cảnh báo sự cố

### Cảnh báo trực tiếp trên màn hình chính



***Hình 3.19. Màn hình hiển thị cảnh báo trên màn hình Dashboard***



***Hình 3.20. Hiển thị chuông cảnh báo***

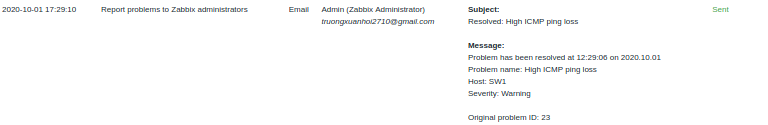
### Cảnh báo qua mail



***Hình 3.21. Cảnh báo qua mail***

Các thông số chúng ta cần quan tâm phần message gửi về bao gồm:

* *Problem:* là biểu hiện của cảnh báo
* *Severity:* mức độ cảnh báo gồm 5 cấp độ: Information, Warning, Average, High, Disaster, trong đó Disaster là cấp độ cao nhất.
* *Time:* là thời điểm nhận được thông báo
* *Status:* là tình trạng thông báo có 3 biểu hiện
* Failed: lỗi không gửi được thông báo
* Sent: đã được gửi đi
* Process: là đang được xử lý
* *Recipient:* ở đây hệ thống được thiết lập gửi thông báo đi tới Admin và địa chỉ gmail là [truongxuanhoi2710@gmail.com](mailto:truongxuanhoi2710@gmail.com)



***Hình 3.22. Chi tiết cảnh báo***

# KẾT LUẬN

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

Đồ án thực hiện thành công mô hình giám sát mạng sử dụng phần mềm Zabbix đáp ứng được cơ bản yêu cầu quả trị mạng của 1 hệ thống bao gồm:

* Quản lý được dữ liệu quan trọng và các thông tin cơ bản của các thiết bị trong hệ thống kịp thời chính xác.
* Xây dựng thành công cơ chế cảnh báo online và hiển thị cảnh báo trên màn hình tiện ích quan trọng cho việc quản trị.

Em đã áp dụng các kiến thức đã học của các môn như quản trị mạng, mạng máy tính, phân tích và thiết kế mạch máy tính, ... vào mô hình và thực tế. Đã học hỏi được thêm nhiều kinh nghiệm về cách 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 em chưa đi sâu tìm hiểu được thêm những những vấn đề cần thiết của hệ thống.

Trong thời gian tới em sẽ phát triển và nghiên cứu sâu hơn về hệ thống giám sát mạng Zabbix và các công cụ hỗ trợ giám sát mạng, giám sát sâu hơn những vấn đề cần thiết của hệ thống. Phát triển các chức năng trên Zabbix như: giám sát hạ tầng mạng bao gồm thiết bị router, switch, firewall, ... Cảnh báo qua SMS.

# TÀI LIỆU THAM KHẢO

[1] <https://news.cloud365.vn/zabbix-cau-hinh-zabbix-server-gui-canh-bao-qua-gmail/>

[2] <https://news.cloud365.vn/zabbix-giam-sat-cisco-switch-snmp/>

[3] <https://news.cloud365.vn/zabbix-giam-sat-server-ubuntu-16-04-bang-zabbix-agent/>

[4] <https://www.zabbix.com/>

[5] <https://www.eve-ng.net/index.php/documentation/>

[6] <https://www.slideshare.net/trongthuy3/luan-van-he-thong-giam-sat-mang-dua-tren-phan-mem-zabbix-hay>