

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**



MÔN HỌC: ĐÁNH GIÁ HIỆU NĂNG HỆ THỐNG MÁY TÍNH

**BÁO CÁO CUỐI KÌ
NHÓM 15**

ĐỀ TÀI: Network traffic monitoring: NagiOS

GVHD: Nguyễn Khánh Thuật

Lớp: NT531.M21

Sinh viên thực hiện

Nguyễn Mỹ Bảo	19521250
---------------	----------

CHƯƠNG 1: MỞ ĐẦU	4
1.1 Lý do chọn đề tài	4
1.2 Mục tiêu đề tài	4
1.3 Nội dung đề tài	5
CHƯƠNG 2: HỆ THỐNG GIÁM SÁT MẠNG.....	6
2.1 Giám sát mạng.....	6
2.1.1 Giám sát mạng là gì ?	6
2.1.2 Các yếu tố cơ bản bên trong giám sát mạng	7
2.1.3 Chức năng của giám sát mạng	7
2.1.4 Tầm quan trọng của giám sát mạng	7
2.2 Hệ thống giám sát mạng	8
2.2.1 Cách hệ thống giám sát mạng hoạt động	8
2.2.2 Mô hình FCAPS (Fault Configuration Accounting Performance Security).....	10
2.2.3 Lợi ích của việc xây dựng hệ thống giám sát mạng	11
CHƯƠNG 3: GIAO THỨC HỖ TRỢ VÀ CÁC THÀNH PHẦN	12
3.1 Giao thức SNMP	12
3.1.1 SNMP là gì ?	12
3.2.2 Các thành phần trong SNMP.....	13
3.2.2.1 Kiến trúc của SNMP	13
3.2.2.2 Object ID.....	14
3.2.2.3 Object Access.....	16
3.2.2.4 Management Information Base	16
3.2.3 Các phiên bản và phương thức của SNMP	18
3.2.3.1 SNMPv1	18
3.2.3.1.1 GetRequest.....	19
3.2.3.1.2 GetNextRequest.....	19
3.2.3.1.3 SetRequest	19
3.2.3.1.4 GetResponse	20
3.2.3.1.5 Trap	20
3.2.3.2 SNMPv2c	22
3.2.3.3 SNMPv2u	22
3.2.3.4 SNMPv3	23
3.2.4 Các cơ chế bảo mật cho SNMP	23

3.2.4.1 Community String.....	23
3.2.4.2 View	24
3.2.4.3 SNMP access control list.....	25
3.2.5. Cấu trúc bản tin của SNMP	25
CHƯƠNG 4: PHẦN MỀM NAGIOS.....	27
4.1 Phần mềm Nagios.....	27
4.1.1 Nagios là gì ?	27
4.1.2 Ứng dụng của Nagios	27
4.1.3 Cấu trúc và cách hoạt động của Nagios	28
4.1.4 Các dịch vụ Nagios cung cấp.....	30
4.1.4.1 Nagios Core.....	31
4.1.4.2 Nagios XI	31
4.1.4.3 Các phần mở rộng (có trả phí) khác của Nagios.....	32
4.1.4.3.1 Nagios Log Server	32
4.1.4.3.2 Nagios Network Analyzer	33
4.1.4.3.3 Nagios Fusion	33
CHƯƠNG 5: TRIỂN KHAI PHẦN MỀM NAGIOS	34
5.1 Mô hình thực nghiệm.....	34
5.2 Cài đặt Nagios XI.....	35
5.3 Giám sát các Client	39
5.3.1 Giám sát Windows bằng SNMP	39
5.3.2 Giám sát Windows Server bằng NCPA	50
5.3.3 Giám sát Windows bằng NSClient++.....	53
5.3.4 Giám sát Router bằng giao thức SNMP.....	57
5.4 Cài đặt Nagios Network Analyzer (Nagios NA)	60
5.4.1 Cài đặt Nagios NA.....	60
5.4.2 Kết nối Nagios NA và Nagios XI.....	60
5.5 Nagios NA phân tích dữ liệu từ Router.....	62
CHƯƠNG 6: TÀI LIỆU THAM KHẢO	65

CHƯƠNG 1: MỞ ĐẦU

1.1 Lý do chọn đề tài

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 việc 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 mạng có hiệu quả như Nagios, Zabbix, Zenoss, Cacti,...

Vì vậy, nhóm em đã chọn đề tài “Hệ thống giám sát mạng sử dụng phần mềm Nagios”, một phần mềm với nhiều chức năng mạnh mẽ cho phép quản lý các thiết bị, dịch vụ trong hệ thống mạng. Với mục tiêu nghiên cứu, tìm hiểu về giải pháp giúp cho mọi người có cái nhìn tổng quan về một hệ thống giám sát mạng hoàn chỉnh.

1.2 Mục tiêu đề tài

Mục tiêu nghiên cứu đề tài của nhóm bao gồm các điểm sau:

- Tìm hiểu hệ thống giám sát mạng
- Tìm hiểu phần mềm Nagios
- Cài đặt và sử dụng phần mềm Nagios

1.3 Nội dung đề tài

Đề hoàn thành các mục tiêu trên, nhóm tập trung nghiên cứu các nội dung sau:

- Nghiên cứu vai trò của hệ thống giám sát mạng
- Nghiên cứu về các giao thức hỗ trợ giám sát mạng
- Nghiên cứu về hệ thống giám sát mạng sử dụng phần mềm Zabbix

CHƯƠNG 2: HỆ THỐNG GIÁM SÁT MẠNG

2.1 Giám sát mạng

2.1.1 Giám sát mạng là gì ?

Giám sát mạng là việc giám sát, theo dõi và ghi nhận những luồng dữ liệu mạng, từ đó sử dụng làm tư liệu để phân tích mỗi khi có sự cố xảy ra.

Giám sát mạng là một chức năng quan trọng, có vai trò giám sát mạng giám sát cho nhiều vấn đề, chẳng hạn như tìm và giúp đỡ giải quyết việc tải trang web snail-paced, mất mát email, hoạt động của người truy vấn - truyền tải file, nguyên nhân quá tải, sự cố server, kết nối mạng delay hoặc các vấn đề thiết bị khác. 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 cần phải nắm rõ được tình hình “sức khỏe” của các thiết bị, dịch vụ được triển khai để có những quyết định xử lý kịp thời và hợp lý nhất. Ngoài ra việc hiểu rõ tình trạng hoạt động của cá 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 các yêu cầu sử dụng của người dung. Việc giám sát hoạt động của các thiết bị mạng, ứng dụng và dịch vụ trong môi trường mạng, với hàng chục hàng tram 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 thông tin cần thiết để người quản trị nắm được hoạt động của hệ thống mạng, đó là hệ thống giám sát mạng.

Các hệ thống giám sát mạng (Network Monitoring System – NMS) thì khác với các hệ thống phát hiện xâm nhập (IDS) hay các hệ thống ngăn ngừa xâm nhập (IPS). Hệ thống giám sát mạng 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 thập 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 thập 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.

2.1.2 Các yếu tố cơ bản bên 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.

2.1.3 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.

2.1.4 Tầm quan trọng của giám sát mạng

Giám sát mạng thực sự là một 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 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 các 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.

2.2 Hệ thống giám sát mạng

2.2.1 Cách hệ thống giám sát mạng hoạt động

Thông thường một mạng máy tính tối thiểu cần có máy chủ (Server), đường truyền, các thiết bị kết nối (Repeater, Hub, Switch, Bridge,...), máy tính người dùng (Client), card mạng (Network Interface Card – NIC) để kết nối các máy tính lại với nhau. Do hệ thống mạng có rất nhiều các thiết bị kết nối nên công tác giám sát càng đóng vai trò quan trọng để có thể duy trì hệ thống mạng hoạt động một cách ổn định, trơn tru và hiệu quả.

Một hệ thống giám sát gồm có nhiều thành phần: Máy trình sát (Sensor), Máy thu thập (Collector), Cơ sở dữ liệu trung tâm và Công cụ phân tích (Analysis tool). Mỗi một thành phần bao gồm các chức năng riêng, cùng các phương pháp thu thập, phân tích và liệt kê nhằm đảm bảo đánh giá và phản hồi sự kiện xảy ra trong hệ thống mạng một cách nhanh chóng và chính xác nhất

- Máy trình sát (Sensor): là những máy trạm làm nhiệm vụ trình sát. Thành phần này sẽ tiếp cận, tương tác với các hệ thống và dịch vụ cần giám sát để nhận biết trạng

thái của những dịch vụ đó. Trong quá trình triển khai hệ thống, thành phần này sẽ được phân tán nằm rải rác nhiều nơi trên mạng để thu thập thông tin từ những nguồn khác nhau như: Tường lửa, Bộ định tuyến, File nhật ký...

- Máy thu thập (Collector): Một điều đáng chú ý trong hệ thống giám sát mạng là các hệ thống, các dịch vụ cần giám sát có thể khác nhau. Điều này đồng nghĩa với việc thông tin thu được cũng có nhiều dạng khác nhau. Để có được thông tin một cách đồng nhất nhằm mục đích xử lý và thống kê, cần có một thành phần làm nhiệm vụ chuẩn hóa thông tin. Máy thu thập sẽ đọc những thông tin thu được từ các máy trình sát và chuẩn hóa thông tin dựa trên những quy tắc chuẩn hóa biết trước. Thông tin đầu ra sẽ có định dạng giống nhau và được lưu vào cơ sở dữ liệu trung tâm.
- Cơ sở dữ liệu trung tâm: là nơi lưu trữ dữ liệu của toàn bộ hệ thống giám sát. Các dữ liệu ở đây đã được chuẩn hóa nên có thể sử dụng để tính toán các số liệu thống kê trên toàn hệ thống
- Công cụ phân tích (Analysis tool): Thành phần này sẽ đọc các dữ liệu từ cơ sở dữ liệu trung tâm và tính toán để tạo ra bản báo cáo số liệu thống kê trên toàn hệ thống.

Việc thu thập dữ liệu ở đây chính là việc lấy các thông tin liên quan đến tình trạng hoạt động của các thiết bị trong hệ thống mạng. Tuy nhiên, trong những hệ thống mạng lớn thì các dịch vụ hay các thiết bị không đặt tại trên máy, một địa điểm mà nằm trên các máy chủ, các hệ thống con riêng biệt nhau. Các thành phần hệ thống cũng hoạt động trên những nền tảng hoàn toàn khác nhau. Có 2 phương pháp để thu thập dữ liệu:

- Phương pháp đẩy: Các sự kiện từ các thiết bị, Các máy trạm, Server sẽ được tự động chuyển về các Collector theo thời gian thực hoặc sau mỗi khoảng thời gian phụ thuộc vào việc cấu hình trên các thiết bị tương ứng. Các Collector của Log Server sẽ thực hiện việc nghe và nhận các sự kiện khi chúng xảy ra.
- Phương pháp kéo: Các Collector thu tập các sự kiện được phát sinh và lưu trữ trên chính các thiết bị và sẽ được lấy về bởi các bộ Collector.

Khi đã thu thập được những thông tin về hệ thống thì công việc tiếp theo là phân tích thông tin, cụ thể là việc thực hiện chỉ mục hóa dữ liệu, phát hiện những điều bất thường,

những mối đe dọa của hệ thống. Dựa trên những thông tin về lưu lượng truy cập, trạng thái truy cập, định dạng request...

Tiếp theo là phát hiện và phản ứng. Phát hiện và phản ứng là hai thành phần quan trọng trong các yếu tố của tiến trình. Sau khi phân tích các thông tin và phát hiện các sự cố liên quan đến phần cứng, phần mềm hay các cuộc tấn công bên ngoài, ta sẽ cần phải nhanh chóng đưa ra giải pháp xử lý sự cố một cách nhanh và hiệu quả nhất.

Sau khi đã thực hiện việc phân tích dữ liệu từ các thông tin thu thập được việc tiếp theo là thực hiện việc đánh giá, đưa thông tin cảnh báo tới người quản trị và thực hiện những công tác nhằm chống lại những mối đe dọa, khắc phục các sự cố có thể xảy ra.

Cảnh báo có thể thông qua email, SMS, hoặc thực thi các mã script nhằm hạn chế hậu quả của sự cố. Khi xảy ra sự cố, hệ thống sẽ tự động gửi email, sms cho người quản trị và cũng có thể chạy script để thêm một địa chỉ IP có biểu hiện tấn công và danh sách đen của Firewall. Việc này đòi hỏi người lập trình phải có hiểu biết sâu và kinh nghiệm về hệ thống.

2.2.2 Mô hình FCAPS (Fault Configuration Accounting Performance Security)

Về yêu cầu khi giám sát hệ thống mạng, ISO (International Organization for Standardization) đã thiết kế một mô hình được gọi là FCAPS nhằm định hướng rõ những việc mà hệ thống giám sát cần phải quản lý. FCAPS là một mô hình quản lý mạng viễn thông và cũng là kiến trúc quản lý mạng. FCAPS sẽ phân nhóm các đối tượng quản lý mạng vào 5 mức (hay mô đun): Fault-management (F), Configuration level (C), Accounting level (A), Performance level (P) và Security level (S).

- **Fault management (Quản lý lỗi):** Các vấn đề mạng được phát hiện và sửa chữa. Các vấn đề tiềm tàng được xác định và có biện pháp để ngăn chặn chúng xảy ra hoặc tái diễn. Với mô đun Fault management, mạng lưới sẽ hoạt động và thời gian chết được giảm tới thiểu.
- **Configuration management (Quản lý cấu hình):** Mô đun này sẽ thực hiện giám sát và kiểm soát hoạt động của mạng lưới. Điều phối các thay đổi về phần cứng và

chương trình, bao gồm cả việc bổ sung thiết bị mới và chương trình mới, sửa đổi các hệ thống hiện có, và xóa bỏ các hệ thống chương trình lỗi thời. Ở mức độ C này, thì tài nguyên của các thiết bị và chương trình được lưu giữ và cập nhật thường xuyên.

- **Accounting management (Quản lý tài khoản):** cũng có thể gọi mô đun này là allocation level, được sử dụng để phân phối các tài nguyên một cách tối ưu và công bằng giữa các người dùng mạng. Điều này giúp sử dụng hiệu quả nhất các hệ thống sẵn có, giảm thiểu chi phí vận hành.
- **Performance management(Quản lý hiệu năng):** liên quan đến việc quản lý toàn bộ hiệu năng của toàn mạng. Thông lượng tối đa, tắc nghẽn mạng và các vấn đề tiềm tàng cần được xác định. Một phần quan trọng khi quản lý hiệu năng là cần mang lại hiệu suất tổng thể lớn nhất.
- **Security management (Quản lý bảo mật):** xử lý và đảm bảo an ninh mạng lưới bởi tin tặc, những người dùng trái phép, hoặc các thiết bị phá hoại. Tính bảo mật thông tin người dùng cần được duy trì được đảm bảo. Hệ thống an ninh cũng cho phép quản trị viên kiểm soát từng cá nhân có thể (và không thể) được làm những gì với hệ thống.

2.2.3 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
- Xác định các điểm thất cổ chai trong hệ thống
- Tìm ra bất thường trong mạng có thể dẫn đến mối đe dọa an ninh

CHƯƠNG 3: GIAO THỨC HỖ TRỢ VÀ CÁC THÀNH PHẦN

3.1 Giao thức SNMP

3.1.1 SNMP là gì ?

SNMP (Simple Network Management Protocol) là một giao thức tầng ứng dụng được Hội đồng Kiến trúc Internet (IAB) xác định trong RFC1157 để trao đổi thông tin quản lý giữa các thiết bị mạng. Nó là một phần của Transmission Control Protocol/Internet Protocol (TCP/IP).

Giao thức SNMP là một trong những giao thức mạng được chấp nhận rộng rãi để quản lý và giám sát các phần tử mạng. Hầu hết các thiết bị mạng được cung cấp đi kèm với SNMP agent. Các agent này phải được kích hoạt và cấu hình để giao tiếp với các công cụ giám sát mạng hoặc hệ thống quản lý mạng (NMS).

SNMP dùng để quản lý, nghĩa là có thể theo dõi, có thể lấy thông tin, có thể được thông báo, và có thể tác động để hệ thống hoạt động như ý muốn. VD 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. 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.

3.2.2 Các thành phần trong SNMP

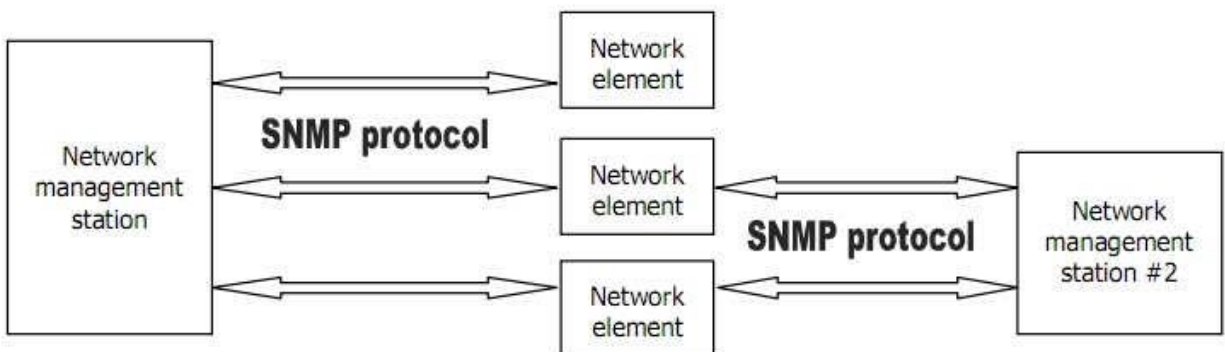
3.2.2.1 Kiến trúc của SNMP

Theo **RFC1157**, kiến trúc của SNMP bao gồm 2 thành phần : các trạm quản lý mạng (network management station) và các thành tố mạng (network element).

Network management station thường là một máy tính chạy phần mềm quản lý SNMP (SNMP management application), dùng để giám sát và điều khiển tập trung các network element.

Network element là các thiết bị, máy tính, hoặc phần mềm tương thích SNMP và được quản lý bởi network management station. Như vậy element bao gồm device, host và application.

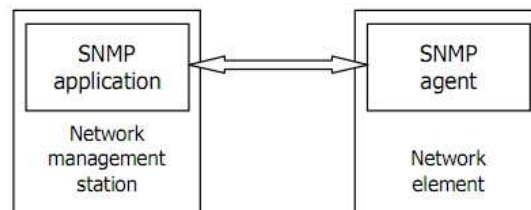
Một management station có thể quản lý nhiều element, một element cũng có thể được quản lý bởi nhiều management station. Vậy nếu một element được quản lý bởi 2 station thì điều gì sẽ xảy ra ? Nếu station lấy thông tin từ element thì cả 2 station sẽ có thông tin giống nhau. Nếu 2 station tác động đến cùng một element thì element sẽ đáp ứng cả 2 tác động theo thứ tự cái nào đến trước.



Hình 1. Kiến trúc của SNMP

Ngoài ra còn có khái niệm SNMP agent. SNMP agent là một tiến trình (process) chạy trên network element, có nhiệm vụ cung cấp thông tin của element cho station, nhờ đó station có thể quản lý được element. Chính xác hơn là application chạy trên station và agent chạy trên element mới là 2 tiến trình SNMP trực tiếp liên hệ với nhau. Các ví dụ minh họa sau đây sẽ làm rõ hơn các khái niệm này :

- Để dùng một máy chủ (= station) quản lý các máy con (= element) chạy HĐH Windows thông qua SNMP thì bạn phải : cài đặt một phần mềm quản lý SNMP (=application) trên máy chủ, bật SNMP service (= agent) trên máy con.
- Để dùng một máy chủ (= station) giám sát lưu lượng của một router (= element) thì bạn phải : cài phần mềm quản lý SNMP (= application) trên máy chủ, bật tính năng SNMP (=agent) trên router.



Hình 2. Hoạt động của SNMP agent

3.2.2.2 Object ID

Một thiết bị hỗ trợ SNMP có thể cung cấp nhiều thông tin khác nhau, mỗi thông tin đó gọi là một *object*. Ví dụ:

- 🌐 Máy tính có thể cung cấp các thông tin : tổng số ổ cứng, tổng số port nối mạng, tổng số byte đã truyền/nhận, tên máy tính, tên các process đang chạy.
- 🌐 Router có thể cung cấp các thông tin : tổng số card, tổng số port, tổng số byte đã truyền/nhận, tên router, tình trạng các port của router,

Mỗi object có một tên gọi và một mã số để nhận dạng object đó, mã số gọi là *Object ID* (OID). Ví dụ:

- ✚ Tên thiết bị được gọi là sysName, OID là 1.3.6.1.2.1.1.5
- ✚ Tổng số port giao tiếp (interface) được gọi là ifNumber, OID là 1.3.6.1.2.1.2.1.
- ✚ Địa chỉ Mac Address của một port được gọi là ifPhysAddress, OID là 1.3.6.1.2.1.2.2.1.6.
- ✚ Số byte đã nhận trên một port được gọi là ifInOctets, OID là 1.3.6.1.2.1.2.2.1.10.

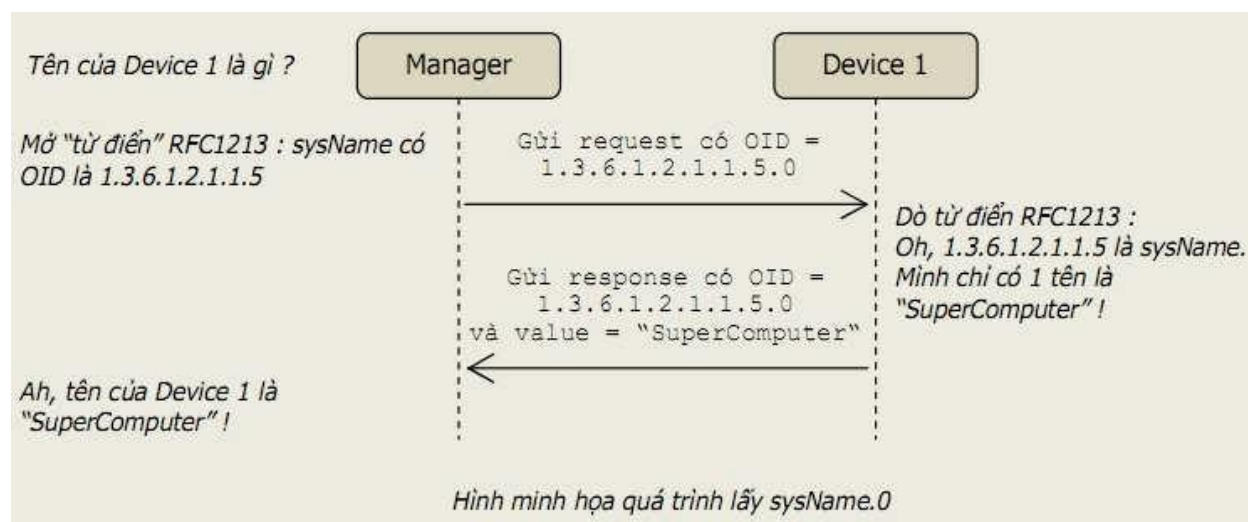
Tuy nhiên nếu một thiết bị lại có nhiều tên thì làm thế nào để phân biệt ? Lúc này người ta dùng thêm 1 chỉ số gọi là “scalar instance index” (cũng có thể gọi là “sub-id”) đặt ngay sau OID. Ví dụ :

- ✚ Tên thiết bị được gọi là sysName, OID là 1.3.6.1.2.1.1.5; nếu thiết bị có 2 tên thì chúng sẽ được gọi là sysName.0 & sysName.1 và có OID lần lượt là 1.3.6.1.2.1.1.5.0 & 1.3.6.1.2.1.1.5.1.
- ✚ Địa chỉ Mac address được gọi là ifPhysAddress, OID là 1.3.6.1.2.1.2.2.1.6; nếu thiết bị có 2 mac address thì chúng sẽ được gọi là ifPhysAddress.0 & ifPhysAddress.1 và có OID lần lượt là 1.3.6.1.2.1.2.2.1.6.0 & 1.3.6.1.2.1.2.2.1.6.1.
- ✚ Tổng số port được gọi là ifNumber, giá trị này chỉ có 1 (duy nhất) nên OID của nó không có phân cấp con và vẫn là 1.3.6.1.2.1.2.1.

OID của các object phổ biến có thể được chuẩn hóa, OID của các object do bạn tạo ra thì bạn phải tự mô tả chúng. Để lấy một thông tin có OID đã chuẩn hóa thì SNMP application phải gửi một bản tin SNMP có chứa OID của object đó cho SNMP agent, SNMP agent khi nhận được thì nó phải trả lời bằng thông tin ứng với OID đó.

Ví dụ: Muốn lấy tên của một PC chạy Windows, tên của một PC chạy Linux hoặc tên của một router thì SNMP application chỉ cần gửi bản tin có chứa OID là 1.3.6.1.2.1.1.5.0. Khi SNMP agent chạy trên PC Windows, PC Linux hay router nhận được bản tin có chứa OID 1.3.6.1.2.1.1.5.0, agent lập tức hiểu rằng đây là bản tin hỏi sysName.0,

và agent sẽ trả lời bằng tên của hệ thống. Nếu SNMP agent nhận được một OID mà nó không hiểu (không hỗ trợ) thì nó sẽ không trả lời.



Hình 3. Quá trình lấy sysName

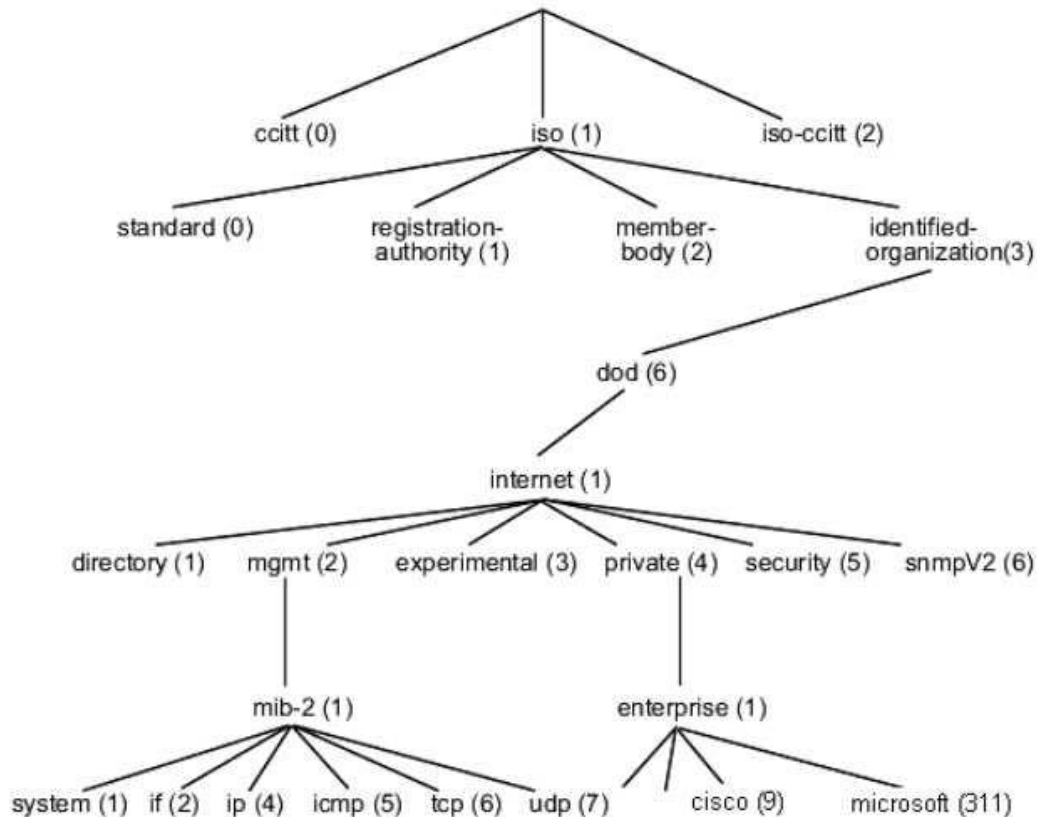
Một trong các ưu điểm của SNMP là nó được thiết kế để chạy độc lập với các thiết bị khác nhau. Chính nhờ việc chuẩn hóa OID mà ta có thể dùng một SNMP application để lấy thông tin các loại device của các hãng khác nhau.

3.2.2.3 Object Access

Mỗi object có quyền truy cập là READ_ONLY hoặc READ_WRITE. Mọi object đều có thể đọc được nhưng chỉ những object có quyền READ_WRITE mới có thể thay đổi được giá trị. VD : Tên của một thiết bị (sysName) là READ_WRITE, ta có thể thay đổi tên của thiết bị thông qua giao thức SNMP. Tổng số port của thiết bị (ifNumber) là READ_ONLY, dĩ nhiên ta không thể thay đổi số port của nó.

3.2.2.4 Management Information Base

MIB (cơ sở thông tin quản lý) là một cấu trúc dữ liệu gồm các đối tượng được quản lý (managed object), được dùng cho việc quản lý các thiết bị chạy trên nền TCP/IP. MIB là kiến trúc chung mà các giao thức quản lý trên TCP/IP nên tuân theo, trong đó có SNMP. MIB được thể hiện thành 1 file (MIB file), và có thể biểu diễn thành 1 cây (MIB tree). MIB có thể được chuẩn hóa hoặc tự tạo.



Hình 4. MIB tree

Một node trong cây là một object, có thể được gọi bằng tên hoặc id. Ví dụ;

- 🚦 Node iso.org.dod.internet.mgmt.mib-2.system có OID là 1.3.6.1.2.1.1, chứa tất cả các object liên quan đến thông tin của một hệ thống như tên của thiết bị (iso.org.dod.internet.mgmt.mib-2.system.sysName hay 1.3.6.1.2.1.1.5).
- 🚦 Các OID của các hãng tự thiết kế nằm dưới iso.org.dod.internet.private.enterprise. Ví dụ : Cisco nằm dưới iso.org.dod.internet.private.enterprise.cisco hay 1.3.6.1.4.1.9, Microsoft nằm dưới iso.org.dod.internet.private.enterprise.microsoft hay 1.3.6.1.4.1.311. Số 9 (Cisco) hay 311 (Microsoft) là số dành riêng cho các công ty do IANA cấp. Nếu Cisco hay Microsoft chế tạo ra một thiết bị nào đó, thì thiết bị này có thể hỗ trợ các MIB chuẩn đã được định nghĩa sẵn (như mib-2) hay hỗ trợ MIB được thiết kế riêng. Các MIB được công ty nào thiết kế riêng thì phải nằm bên dưới OID của công ty đó.

3.2.3 Các phiên bản và phương thức của SNMP

SNMPv1 có 5 phương thức, tuy nhiên các version khác sau này được bổ sung thêm một số phương thức mới và sẽ khác nhau ở cấu trúc các bản tin.

3.2.3.1 SNMPv1

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.

Bảng 1. Tác dụng của các phương thức SNMPv1

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.

3.2.3.1.1 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. Ví dụ: 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.

3.2.3.1.2 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. 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.

3.2.3.1.3 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

Chỉ những object có quyền READ_WRITE mới có thể thay đổi được giá trị.

3.2.3.1.4 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.

3.2.3.1.5 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.

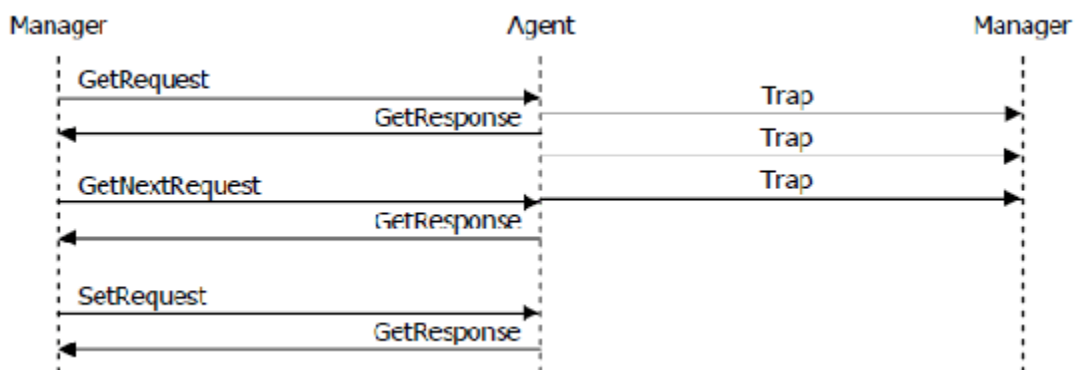
Phương thức trap là độc lập với các phương thức request/response. SNMP request/response dùng để quản lý còn SNMP trap dùng để cảnh báo. Nguồn gửi trap gọi là Trap Sender và nơi nhận trap gọi là Trap Receiver. Một trap sender có thể được cấu hình để gửi trap đến nhiều trap receiver cùng lúc.

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.

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” 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.



Hình 5. Các phương thức của 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.

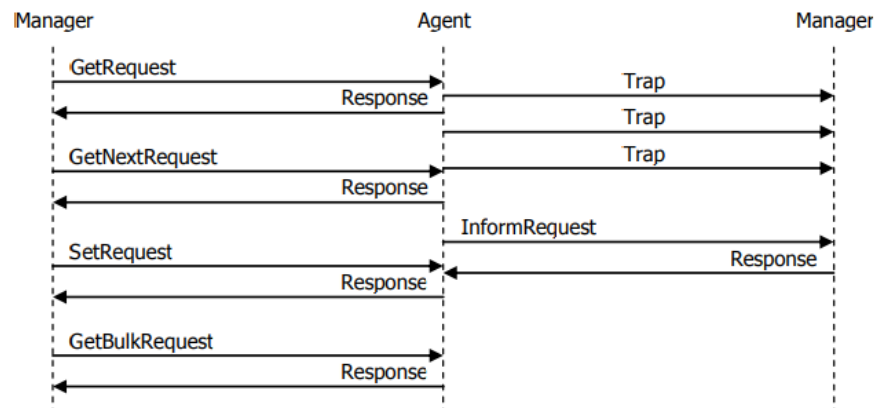
3.2.3.2 SNMPv2c

SNMP version 2 chia thành 2 phiên bản khác nhau ở cơ chế bảo mật, trong đó phiên bản vẫn sử dụng cơ chế bảo mật dựa vào community string như ở SNMPv1 gọi là Community-based SNMPv2 hay SNMPv2c. Một số tài liệu đã ghi chú không đúng rằng “SNMPv2c bổ sung thêm cơ chế community string so với SNMPv1”, thực sự SNMPv2c và SNMPv1 đều có cơ chế xác thực đơn giản bằng community giống nhau.

Khác biệt của SNMPv2c so với SNMPv1 là :

- Có nhiều phương thức hơn so với SNMPv1.
- Cấu trúc bản tin Trap PDU khác so với SNMPv1.
- Có thêm bản tin Bulk PDU với cấu trúc riêng.

SNMPv2c có 8 phương thức gồm : GetRequest, GetNextRequest, Response, SetRequest, GetBulkRequest, InformRequest, Trap và Report. Như vậy so với SNMPv1 thì v2c có thêm các phương thức GetBulk, Inform và Report.



Hình 6. Các phương thức của SNMPv2c

3.2.3.3 SNMPv2u

Đây là phiên bản SNMPv2 sử dụng cơ chế bảo mật có chứng thực bằng băm1 và mã hóa đối xứng2 dữ liệu, gọi là User-based SNMPv2 hay SNMPv2u. Sau này phiên bản SNMPv3 ra đời đã thay thế hoàn toàn SNMPv2u và người ta không còn ưu tiên dùng

SNMPv2u nữa. Do đó SNMPv2u sẽ không được trình bày trong tài liệu này mà SNMPv3 sẽ được trình bày chi tiết. Trong thực tế rất khó tìm thấy một thiết bị còn hỗ trợ SNMPv2u.

3.2.3.4 SNMPv3

Phiên bản bảo mật nhất của SNMP sử dụng mô hình bảo mật dựa trên người dùng (User-based security model) với các cơ chế chứng thực bằng băm (MD5, SHA) và mã hóa (DES, AES) hiện đại. Việc lập trình ứng dụng hỗ trợ được SNMPv3 phức tạp hơn, do đó hầu hết các phần mềm SNMP manager phiên bản có hỗ trợ SNMPv3 đều có tính phí, trong khi phiên bản miễn phí chỉ hỗ trợ SNMPv1 và SNMPv2.

3.2.4 Các cơ chế bảo mật cho SNMP

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.

3.2.4.1 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.

3.2.4.2 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 ma

nager 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.

3.2.4.3 SNMP access control list

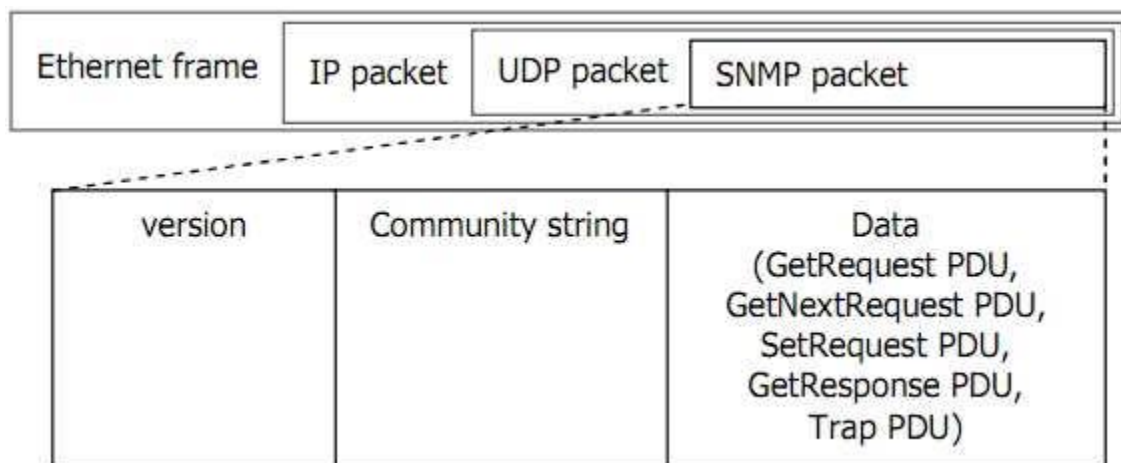
Khi manager gửi không đúng community hoặc khi OID cần lấy lại không nằm trong view cho phép thì agent sẽ không trả lời. Tuy nhiên khi community bị lộ thì một manager nào đó vẫn request được thông tin. Để ngăn chặn hoàn toàn các SNMP manager không được phép, người quản trị có thể dùng đến SNMP access 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

3.2.5. Cấu trúc bản tin của SNMP

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



Hình 7. 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 4: PHẦN MỀM NAGIOS

4.1 Phần mềm Nagios

4.1.1 Nagios là gì ?

Nagios là một hệ thống giám sát mã nguồn mở cho các hệ thống máy tính. Nó được thiết kế để chạy trên hệ điều hành Linux và có thể giám sát các thiết bị chạy hệ điều hành Linux, Windows và Unix (OSes).

Phần mềm Nagios chạy kiểm tra định kỳ về các thông số quan trọng của tài nguyên ứng dụng, mạng và máy chủ. Ví dụ: Nagios có thể theo dõi việc sử dụng bộ nhớ, sử dụng đĩa, tải bộ vi xử lý, số lượng quy trình hiện đang chạy và tệp nhật ký. Nagios cũng có thể giám sát các dịch vụ, chẳng hạn như Giao thức gửi thư đơn giản (SMTP), Giao thức Mail 3 (POP3), Giao thức truyền siêu văn bản (HTTP) và các giao thức mạng phổ biến khác. Nagios có thể tự kiểm tra chủ động, và cũng có thể chạy kiểm tra khi nhận được lệnh từ các phần mềm quản lý khác

Ban đầu được gọi là NetSaint và phát hành vào năm 1999, Nagios được phát triển bởi Ethan Galstad và sau đó được tinh chỉnh bởi nhiều người đóng góp như một dự án nguồn mở. Nagios Enterprises, một công ty dựa trên công nghệ Nagios Core, đã sử dụng công cụ mã nguồn mở này để cung cấp nhiều sản phẩm, chẳng hạn như XI, Log Server, Network Analyzer và Fusion. Tất cả đều thuộc về hệ sinh thái của Nagios và có các ứng dụng chuyên biệt khác nhau trong từng lĩnh vực

4.1.2 Ứng dụng của Nagios

Dù hoạt động chủ yếu trong lĩnh vực quản lý hệ thống mạng máy tính, như đã nói trên, Nagios có rất nhiều phần mềm trong hệ sinh thái, và mỗi phần mềm lại chuyên trách một nhiệm vụ khác nhau trong việc quản lý này.

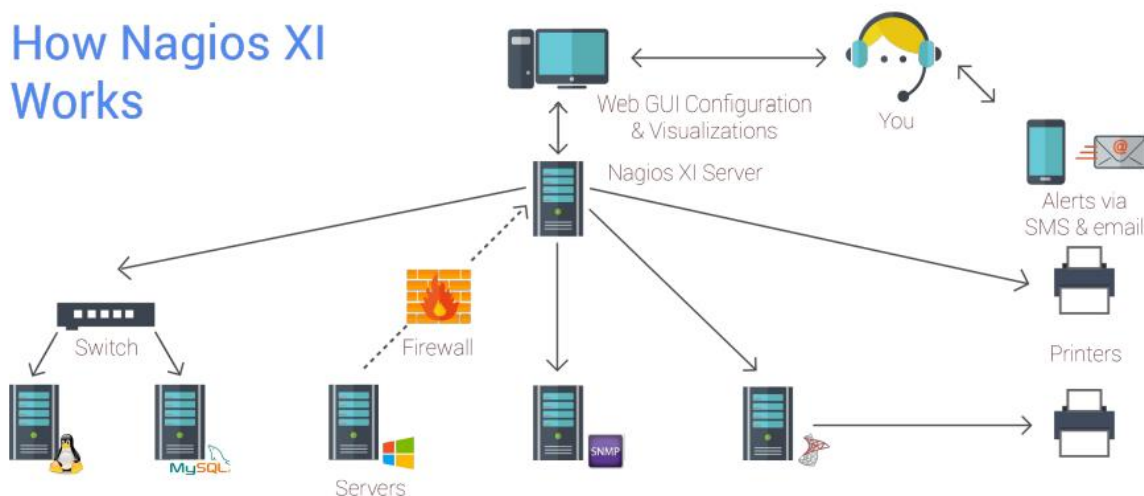
Những công dụng có thể kể đến của Nagios là:

- Xác định tất cả các loại vấn đề máy chủ và mạng đang gặp phải; giúp quản trị viên hệ thống phân tích nguyên nhân gốc rễ của vấn đề. Vì vậy, người dùng có thể đưa ra một giải pháp lâu dài cho các vấn đề thường xuyên xảy ra.
- Sàng lọc toàn bộ quy trình vận hành và cơ sở hạ tầng đầu cuối và cho phép người dùng khắc phục sự cố của máy chủ khi gặp vấn đề về hiệu suất. Nó cũng giúp người dùng lập kế hoạch phân bổ cơ sở hạ tầng hệ thống mạng của mình và cập nhật nó cho phù hợp, tránh việc các ứng dụng không được cập nhật và gây ra lỗi. Nagios sử dụng một đường truyền duy nhất để giám sát toàn bộ cơ sở hạ tầng.
- Việc bảo trì và bảo mật của máy chủ có thể được tiêu chuẩn hóa và quản lý bởi Nagios; thậm chí là tự động khắc phục các sự cố, ngay cả trong các tình huống quan trọng. Nếu có bất kỳ biến động nào trong hệ thống, nó sẽ kích hoạt cảnh báo để ngăn chặn các tình huống tệ hơn có thể gây ra do thao tác sai trong tình huống cấp bách. Do đó, Nagios tương đối an toàn, có thể quản lý và có thể mở rộng.
- Nagios có một cơ sở dữ liệu đáng tin cậy và một hệ thống theo dõi nhật ký hiệu quả với các giao diện web trực quan.
- Kiến trúc của sản phẩm rất đơn giản. Nagios hoạt động bằng cách mã hóa các plugin mới với đa dạng các ngôn ngữ có thể phục vụ cho hệ thống.
- Nagios được sử dụng cho các dịch vụ mạng giám sát định kỳ như SMTP, HTTP, NNTP, ICMP, FTP, POP, SNMP, v.v. Nagios, bằng cách sử dụng một máy chủ làm máy chủ mẹ (máy chủ root), có thể xác định hệ thống phân cấp của máy chủ mạng.

4.1.3 Cấu trúc và cách hoạt động của Nagios

Nagios dựa trên kiến trúc client - server để tạo thành một mạng lưới. Nagios được thực thi trên máy chủ và các plugin điều khiển được kích hoạt trên tất cả các máy chủ từ xa cần được theo dõi định kỳ.

How Nagios XI Works



Bộ lập lịch là một thành phần quan trọng trong hệ thống Nagios. Chỉ có sử dụng bộ lập lịch, ta mới có thể truyền tín hiệu để chạy các plugin tại một vị trí từ xa (remote). Plugin này hoàn toàn nhận được trạng thái của máy chủ từ xa. Sau đó, thông tin được gửi đến bộ lập lịch trình quá trình từ plugin. Bộ lập lịch quy trình liên tục cập nhật GUI (giao diện người dùng), sau đó thông báo được gửi đến quản trị viên để cho họ biết tình trạng hiện tại của hệ thống mạng.

Giao diện điều khiển của Nagios cũng đa dạng. Người dùng có thể chọn làm việc trong giao diện dòng lệnh (CLI) hoặc chọn giao diện người dùng đồ họa dựa trên web (GUI) (riêng GUI sẽ chỉ có trong một số phiên bản của Nagios từ các bên thứ ba, ví dụ như của Nagios Enterprises). Bảng điều khiển của Nagios cung cấp một cái nhìn tổng quan về các thông số quan trọng được theo dõi trên toàn bộ hệ thống.

Dựa trên các thông số và ngưỡng được xác định, Nagios có thể gửi cảnh báo nếu đạt đến mức nào đó (được thiết lập trước bởi admin). Những thông báo này có thể được gửi theo những cách khác nhau, bao gồm email và tin nhắn văn bản. Ngoài ra, ta còn có thể phân quyền truy cập cho những người có thể truy cập hệ thống

Nagios chạy cả cấu hình trên các Software agent - giám sát tác tử, và Software agentless - giám sát không tác tử. Các tác tử độc lập được cài đặt trên bất kỳ hệ thống phần

cứng hoặc phần mềm nào để thu thập dữ liệu sau đó được báo cáo lại cho máy chủ quản lý. Giám sát không tác tử sử dụng các giao thức hiện có để mô phỏng một tác tử (nói một cách ngắn gọn, giám sát phần mềm một cách tự động không cần có một tác tử nào tác động vào hệ thống). Cả hai cách tiếp cận đều có thể theo dõi việc sử dụng hệ thống tệp, số liệu hệ điều hành, trạng thái dịch vụ và quy trình và hơn thế nữa.

Ví dụ về các agent (tác tử) Nagios bao gồm Nagios Remote Data Processor (NRDP), Nagios Cross Platform Agent (NCPA) và NSClient ++. Nagios cũng có thể chạy các tập lệnh và plugin từ xa bằng cách sử dụng agent Nagios Remote Plugin Executor (NRPE). NRPE cho phép giám sát từ xa các số liệu hệ thống như tải hệ thống, bộ nhớ và tình trạng RAM, disk,... Nó bao gồm check_nrpe plug-in, được lưu trữ trên máy giám sát cục bộ và NRDP, chạy trên máy chủ remote. Nagios sử dụng một plugin để hợp nhất dữ liệu từ tác nhân NRPE trước khi nó đi đến máy chủ quản lý để xử lý. NRPE cũng có thể giao tiếp với các agent Windows để giám sát các máy Windows.

Nagios hỗ trợ các plugin là các tiện ích bổ sung và tiện ích mở rộng độc lập để người dùng có thể xác định mục tiêu và thông số muốn theo dõi. Nagios plugin xử lý các đối số dòng lệnh và truyền các lệnh này tới Nagios Core. Có khoảng 50 plugin được phát triển và duy trì bởi Nagios, và hơn 3.000 plugin từ cộng đồng. Các plugin cũng khá đa dạng về mặt hình thức, bao gồm phần cứng, phần mềm, đám mây, OSes, bảo mật, tệp nhật ký và kết nối mạng. Ví dụ, khi được sử dụng kết hợp với các hệ thống cảm biến môi trường, plug-in Nagios có thể chia sẻ dữ liệu về các biến môi trường, chẳng hạn như nhiệt độ, độ ẩm hoặc áp suất khí quyển.

4.1.4 Các dịch vụ Nagios cung cấp

Nagios đã được chứng minh là phổ biến trong các doanh nghiệp nhỏ và lớn, cũng như các nhà cung cấp dịch vụ internet (ISP), các tổ chức giáo dục, cơ quan chính phủ, tổ chức chăm sóc sức khỏe, công ty sản xuất và tổ chức tài chính.

Người dùng có thể chọn tùy chọn miễn phí và trả phí, tùy thuộc vào các dịch vụ và hỗ trợ cần thiết.

4.1.4.1 Nagios Core

Dịch vụ này ban đầu có tên là Nagios, và bây giờ được gọi là Nagios Core. Core có sẵn và miễn phí như một phần mềm giám sát nguồn mở cho các hệ thống CNTT, mạng và cơ sở hạ tầng. Tương tự như Linux, người ta phát triển các phần mềm riêng biệt (distro) dựa trên Core. Core chứa một loạt các giám sát cơ sở hạ tầng thông qua việc cho phép các plug-in mở rộng khả năng giám sát của nó. Đây là cơ sở cho các hệ thống giám sát Nagios trả tiền.

Nagios Core có giao diện web tùy chọn, hiển thị trạng thái mạng, thông báo, tệp nhật ký và hơn thế nữa. Core có thể thông báo cho người dùng của mình khi có vấn đề về máy chủ hoặc máy khách. Ngoài ra, Core có thể giám sát các dịch vụ mạng như SMTP, HTTP và Ping.

4.1.4.2 Nagios XI

Nagios XI là một giao diện mở rộng của Nagios Core, được xem là phiên bản cấp doanh nghiệp của công cụ giám sát. XI hoạt động như phần mềm giám sát, trình quản lý cấu hình và bộ công cụ. Trong khi Nagios Core miễn phí, XI có tính phí, và được phát hành bởi Nagios Enterprises. Ngoài các tính năng tương tự như Core, XI bổ sung các máy ảo được cấu hình sẵn (VMs), giao diện người dùng cấu hình web (UI), đồ thị hiệu suất, ứng dụng di động, bảng điều khiển, báo cáo theo lịch trình, hỗ trợ kỹ thuật qua email và hơn thế nữa.

Nagios XI giám sát các thành phần cơ sở hạ tầng CNTT như ứng dụng, OSes, mạng và số liệu hệ thống. Plugin được hỗ trợ cho các thành phần cơ sở hạ tầng này để mở rộng khả năng giám sát của XI.

Bảng dưới đây cung cấp các đề xuất phần cứng dựa trên tỷ lệ (máy chủ) trên dịch vụ là 1: 5

Monitored Nodes / Hosts	Monitored Services	Hard Drive Space	CPU Cores	RAM
50	250	40 GB	1 – 2	1 – 4 GB
100	500	80 GB	2 – 4	4 - 8 GB
> 500	> 2500	120 GB	> 4	> 8GB

Đối với các cài đặt giám sát hơn 1000 máy chủ hoặc 5000 dịch vụ, thường được khuyên các admin nên cài đặt Nagios XI trên máy chủ vật lý thay vì máy ảo. Do tài nguyên phần cứng được chia sẻ và cách VM xử lý quá trình phân nhánh, các máy ảo có thể không đáp ứng được phần cứng nhu cầu của môi trường lớn ngay cả với các cải tiến về hiệu suất.

4.1.4.3 Các phần mở rộng (có trả phí) khác của Nagios.

4.1.4.3.1 Nagios Log Server

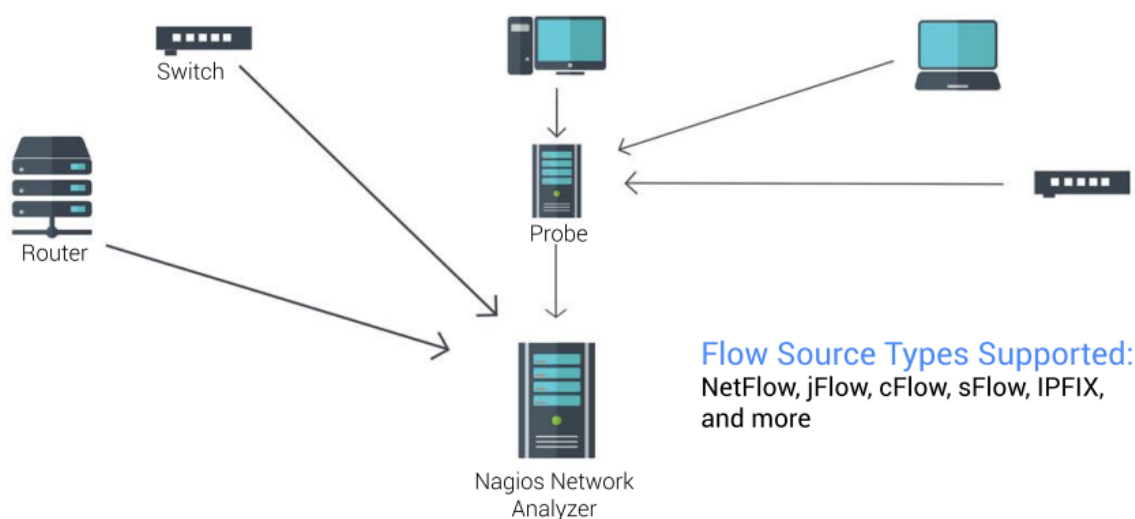
Nagios Log Server là một công cụ quản lý và giám sát nhật ký cho phép một tổ chức xem, sắp xếp và cấu hình nhật ký từ cơ sở hạ tầng CNTT của mình, bao gồm nhật ký sự kiện Windows. Log Server có thể phân tích, thu thập và lưu trữ dữ liệu đã đăng nhập dựa trên các thông số kỹ thuật tùy chỉnh và được chỉ định trước. Người quản trị có thể đặt cảnh báo để thông báo cho người dùng Log Server khi có mối đe dọa tiềm ẩn hoặc trục trặc trên tài sản được giám sát. Ví dụ: cảnh báo sẽ được gửi đến người quản trị Microsoft

Exchange khi có ba lần đăng nhập thất bại vào Exchange Server, có nghĩa là có thể có một người đáng ngờ đang cố gắng đoán mật khẩu cho hệ thống.

4.1.4.3.2 Nagios Network Analyzer

Network Analyzer nhận luồng dữ liệu mạng (netflow data) từ router, switch hoặc đầu dò phần mềm trên toàn bộ cơ sở hạ tầng CNTT của bạn. Các thiết bị này được xác định làm nguồn, lần lượt được phân tích bởi máy chủ Network Analyzer để cung cấp các biểu đồ quan trọng và trực quan hóa dữ liệu.

Network Analyzer cũng có thể xác định xem thông tin về băng thông và luồng có phản ánh hoạt động mạng bình thường hay không. Network Analyzer cung cấp cho quản trị viên hệ thống và người quản lý CNTT các cảnh báo về hành vi bất thường, cho phép phản ứng nhanh với các vi phạm bảo mật hoặc hoạt động bất thường khác.



4.1.4.3.3 Nagios Fusion

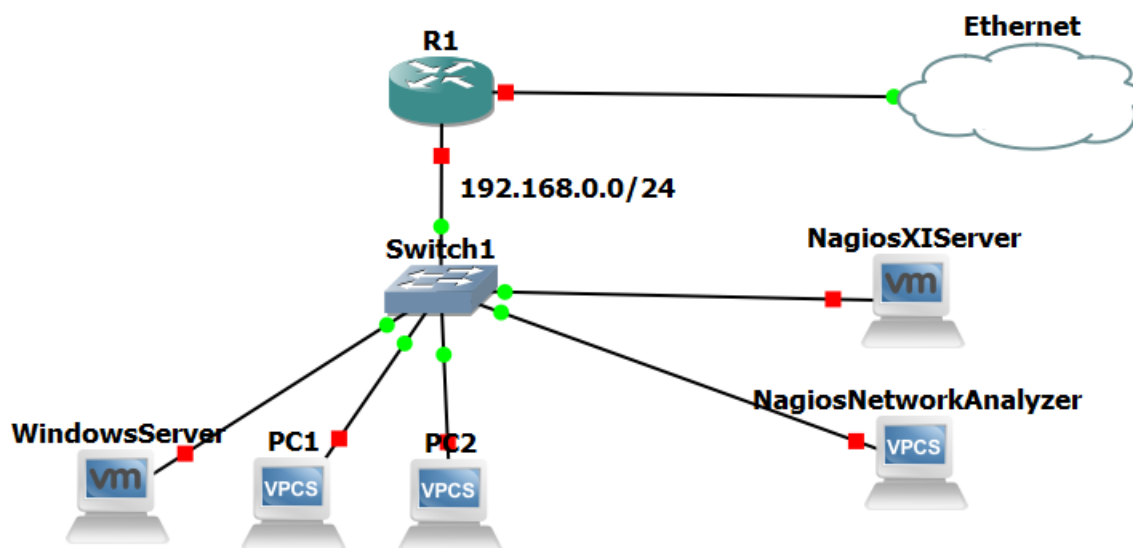
Nagios Fusion là một dịch vụ tổng hợp cho các máy chủ Nagios Core và Nagios XI, hiển thị nhiều hệ thống trong một chế độ xem. Fusion cô đọng quản lý mạng bằng cách tập trung các tính năng và dữ liệu từ XI và Core ở một vị trí. Điều này cho phép người quản

trị hệ thống có một cái nhìn chi tiết về cơ sở hạ tầng mạng. Với Fusion, người quản trị có thể chỉ định máy chủ XI và Core nào được hiển thị và quản lý người dùng nào được phép xem các máy chủ đó. Ngoài ra, người dùng Fusion có thể đăng nhập vào bất kỳ máy chủ được quản lý nào và sử dụng dữ liệu được lưu trữ hoặc trực tiếp để cấu hình biểu đồ và đồ họa khác để xuất hiện trên bảng điều khiển.

CHƯƠNG 5: TRIỂN KHAI PHẦN MỀM NAGIOS

5.1 Mô hình thực nghiệm

Để có thể xây dựng hệ thống thực nghiệm triển khai phần mềm Nagios, nhóm đã sử dụng GNS3 để có thể giả lập hệ thống cùng VMWare để có thể triển khai các client cũng như server.



Tên	Địa chỉ
Nagios XI	192.168.0.197
Nagios Analyzer	192.168.0.196
Router - Interface fa0/0	192.168.0.124
PC1	192.168.0.100
PC2	192.168.0.130
Windows Server	192.168.0.166

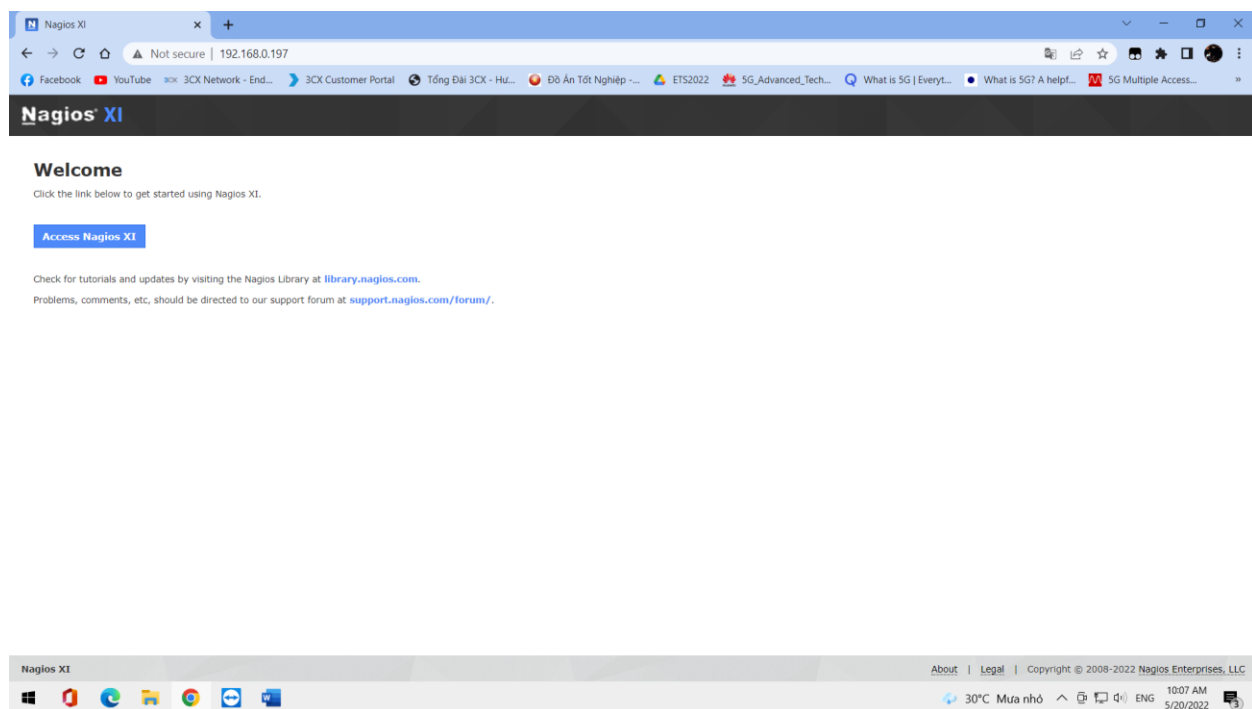
5.2 Cài đặt Nagios XI

Nagios XI được hỗ trợ để có thể chạy trên ba nền tảng là: Microsoft, VMWare và Linux server và ở đồ án này, nhóm sẽ chọn cài đặt Nagios chạy trên nền tảng VMWare. Để có thể tải Nagios XI ta có truy cập đường link sau: <https://www.nagios.com/downloads/nagios-xi/>

Sau khi cài đặt gói ova của Nagios XI về, ta import vào VMWare và chỉ việc power on máy ảo là có thể chạy một Nagios XI server.



Bước 1: Sau khi khởi chạy thành công Server, ta có thể truy cập địa chỉ được cung cấp để tiến hành cài đặt Server và nhấn Access nagios XI.



Bước 2: Tiếp theo, chúng ta cần cấu hình các trường cần thiết và điền license key. Ta có thể sử dụng bản free hoặc bản trial có thời hạn.

The screenshot shows the Nagios XI installation interface. The top navigation bar includes the Nagios XI logo and an 'Install' link. The main content area is divided into two sections: 'General System Settings' and 'License Settings'. In the 'General System Settings' section, there are input fields for 'Program URL' (http://192.168.0.197/nagiosxi/), 'Timezone' (UTC+07:00 Hanoi), 'Language' (English (English)), and 'User Interface Theme' (Modern). There is also a checkbox for 'Use HTTPS only (all HTTP requests will be redirected to HTTPS)'. The 'License Settings' section shows 'License Type' with radio buttons for 'Trial' (selected), 'Licensed', and 'Free (Limited)'. Below this, it states 'Trial includes unlimited nodes + enterprise features. Includes access to trial support.' and provides a link 'Click to get a trial key'. The 'Trial Key' field contains the value 'NTE3N2A0NTKyNzgxNDQx'. The bottom of the page shows a footer with 'Nagios XI', 'About', 'Legal', 'Copyright © 2008-2022 Nagios Enterprises, LLC', and system information like '30°C Mưa nhỏ' and '10:08 AM 5/20/2022'.

Bước 3: Cài đặt các thông tin cần thiết đối với tài khoản admin và nhấn finish install để hoàn tất cài đặt (quá trình hoàn tất tốn một vài phút).

The screenshot shows the 'Nagios XI Installation' page. The top navigation bar includes the Nagios XI logo and an 'Install' link. The main content area is titled 'Nagios XI Installation' and includes a subtitle 'Finalize your Nagios XI installation and step the initial configuration. These settings can be changed later.' Below this, there are two sections: 'Admin Account Settings' and 'Admin Notification Settings'. In the 'Admin Account Settings' section, there are input fields for 'Username' (nagiosadmin), 'Password' (1), 'Full Name' (Nagios Administrator), and 'Email Address' (anhquachh@gmail.com). The 'Admin Notification Settings' section has a checkbox for 'Send this account email notifications' which is checked, and a link for 'Advanced email notification settings'. At the bottom, there are two buttons: '< Back' and 'Finish Install'.

Bước 4: Đăng nhập bằng tài khoản admin đã được cấu hình tại bước 3


Nagios XI Login

Login

Login

Forgot your password?

Select Language:



Nagios XI™

Nagios Products

XI

F

LS

NA

Nagios XI

Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party add-ons provide for monitoring of virtually all in-house applications, services, and systems.

Contact Us

Looking for more information? Have a technical or sales question?

Sales
Phone: (651) 204-9102
Email: sales@nagios.com

Web
[Nagios Website](#)
[Nagios Exchange](#)

Support
[Support Forum](#)
[Knowledgebase](#)

Giao diện Web Interface của Nagios XI server

Nagios XI Home Views Dashboards Reports Configure Tools Help Admin

Notice: This trial copy of Nagios XI will expire in 30 days. [Purchase a License Now](#) or [Enter your license key](#).

Quick View

- Home Dashboard
- Tactical Overview
- Birdseye
- Operations Center
- Operations Screen
- Open Service Problems
- Open Host Problems
- All Service Problems
- All Host Problems
- Network Outages

Details

- Service Status
- Host Status
- Hostgroup Summary
- Hostgroup Overview
- Hostgroup Grid
- Servicegroup Summary
- Servicegroup Overview
- Servicegroup Grid
- BPI
- Metrics

Graphs

- Performance Graphs
- Graph Explorer

Maps

- World Map
- BBmap
- Hypermap
- Minimap

Home Dashboard

Getting Started Guide

Common Tasks:

- [Change your account settings](#)
Change your account password and general preferences.
- [Change your notifications settings](#)
Change how and when you receive alert notifications.
- [Configure your monitoring setup](#)
Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- [Learn about XI](#)
Learn more about XI and its capabilities.
- [Signup for XI news](#)
Stay informed on the latest updates and happenings for XI.

Host Status Summary

Up	Down	Unreachable	Pending
12	0	0	0
Unhandled		Problems	
0		1	

Last Updated: 2022-05-20 10:22:15

Service Status Summary


Ok	Warning	Unknown	Critical	Pending
12	0	0	0	0
Unhandled		Problems		All
0		0		12

Last Updated: 2022-05-20 10:22:15


We're Here To Help!


Our knowledgeable techs are happy to help you with any questions or problems you may have getting Nagios up and running.

[Support Forum / Customer Support Forum](#)
[Help Resources](#)
[Customer Ticket Support Center](#)
[Customer Phone Support: +1 651-204-9102 Ext. 4](#)



Start Monitoring

 Run a Config Wizard

 Run Auto-Discovery

Administrative Tasks

Task

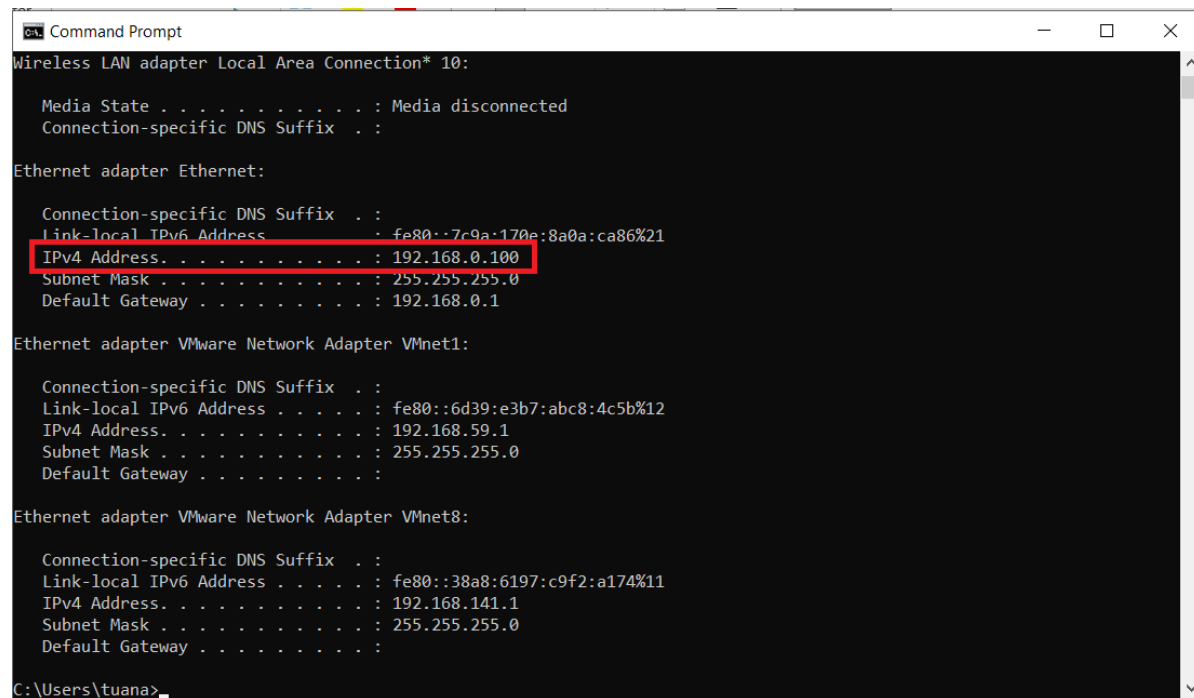
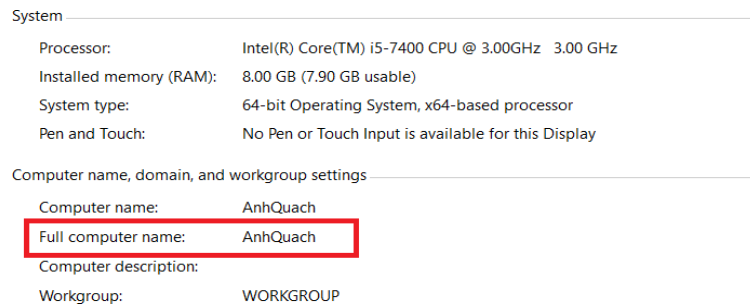
Initial Setup Tasks:

5.3 Giám sát các Client

5.3.1 Giám sát Windows bằng SNMP

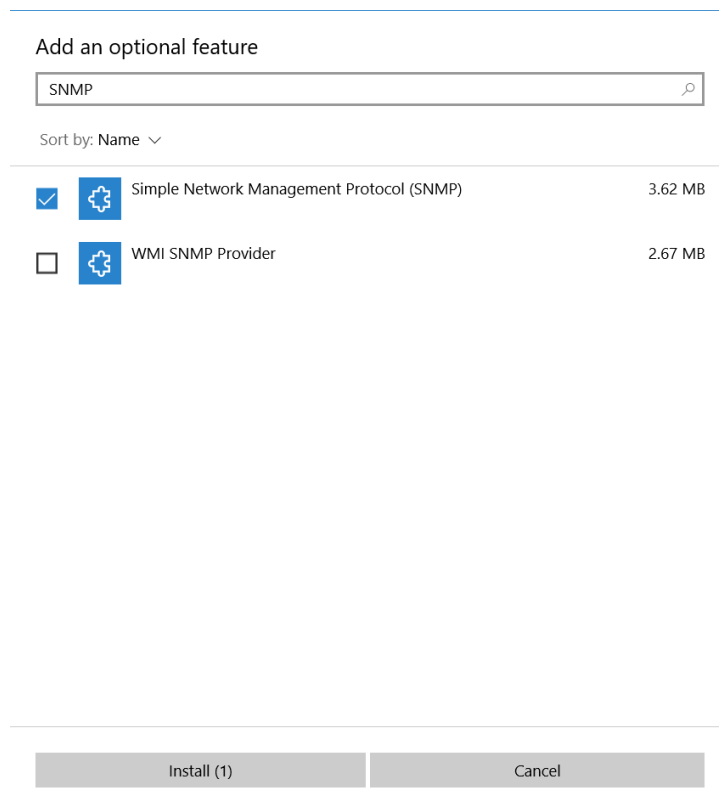
Để có thể giám sát Windows thông qua giao thức SNMP, ta cần phải cài đặt dịch vụ SNMP trên Windows.

Bước 1: Kiểm tra hostname và địa chỉ IP của máy Windows

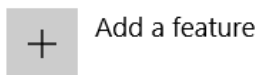


Bước 2: Cài đặt dịch vụ SNMP trên Windows

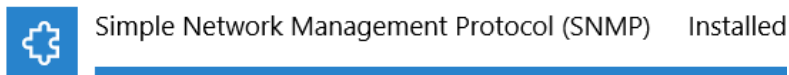
Vào Settings → Apps → Apps & features → Optional feature → Add a feature và tìm kiếm “SNMP”



Optional features



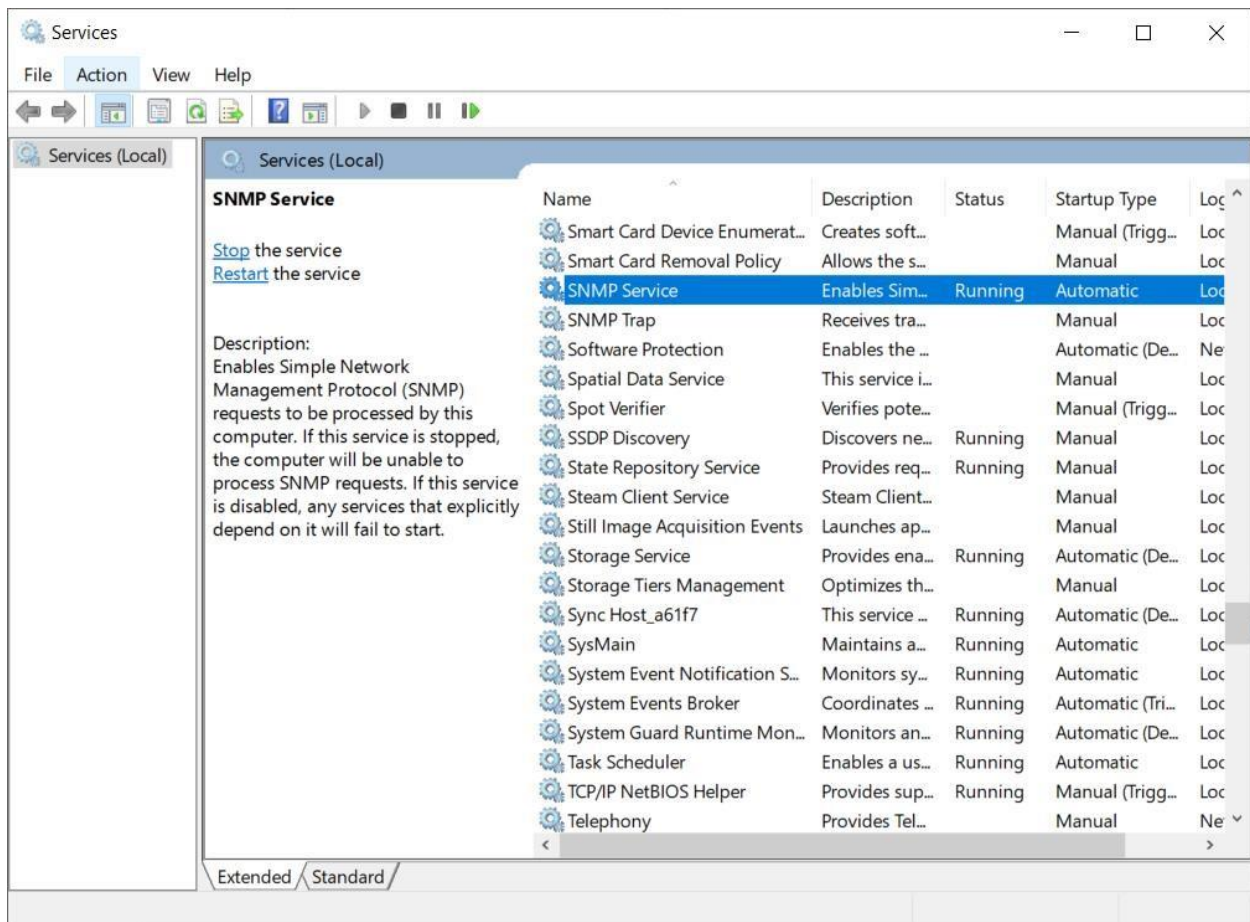
Latest actions



[See optional feature history](#)

Bước 3: Cấu hình dịch vụ SNMP

Vào Services trên Windows và mở SNMP Service



Chọn mục Agent và stick vào tất cả các Service

SNMP Service Properties (Local Computer) X

General Log On Recovery Agent Traps Security Dependencies

Internet management systems may request the contact person, system location, and network services for this computer from the SNMP service.

Contact:

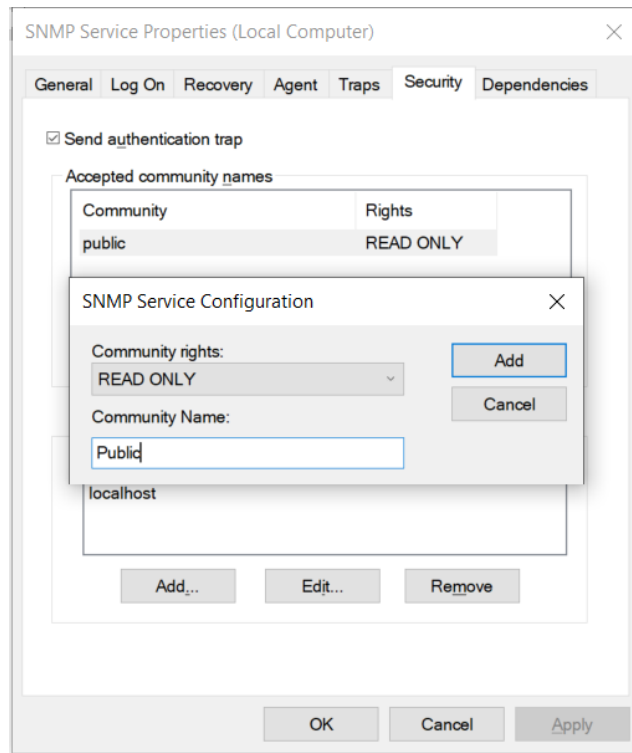
Location:

Service

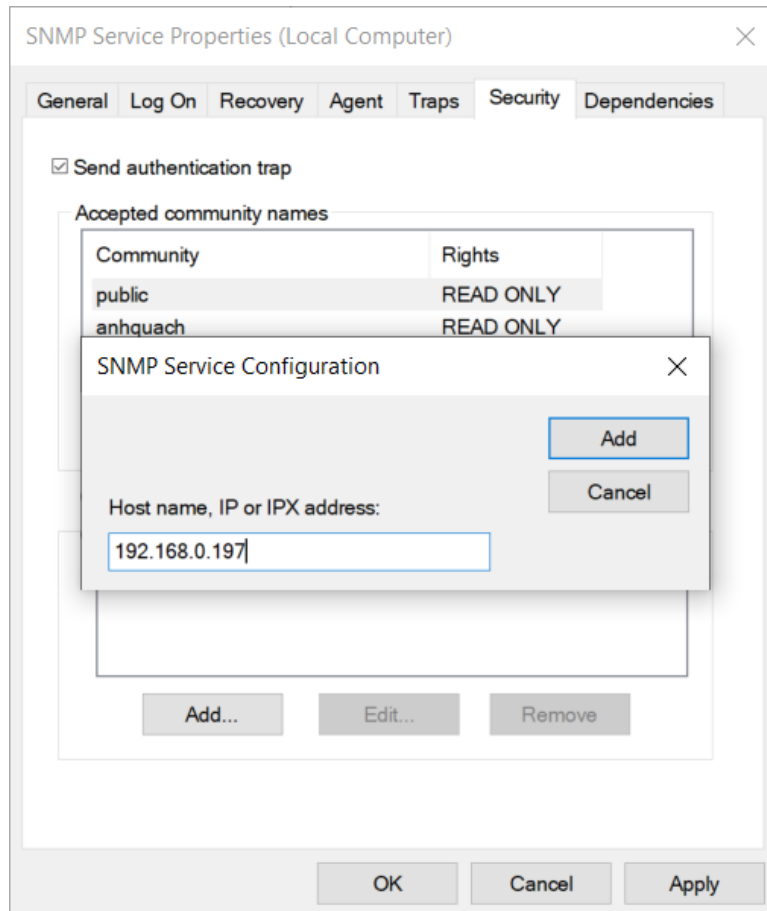
<input checked="" type="checkbox"/> Physical	<input checked="" type="checkbox"/> Applications	<input checked="" type="checkbox"/> Datalink and subnetwork
<input checked="" type="checkbox"/> Internet	<input checked="" type="checkbox"/> End-to-end	

OK Cancel Apply

Vào mục Security → Add Accepted community names

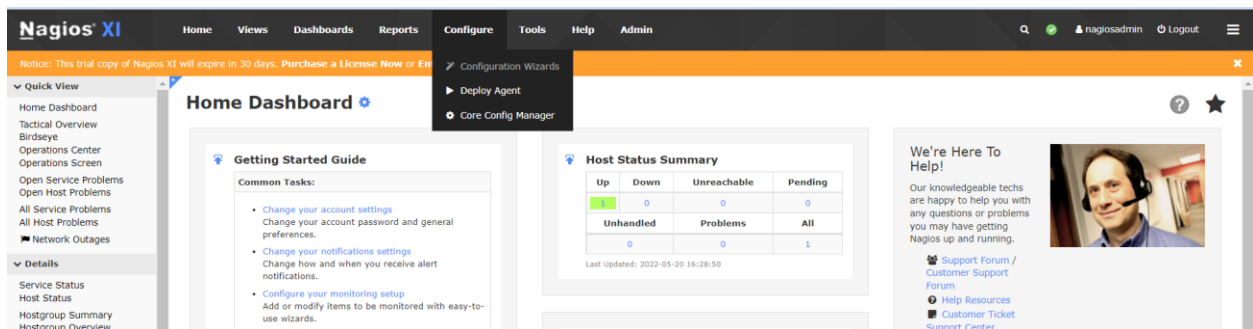


Vào mục Security → chọn “Accept SNMP packets from these hosts” → Add địa chỉ IP của NagiosXI Server

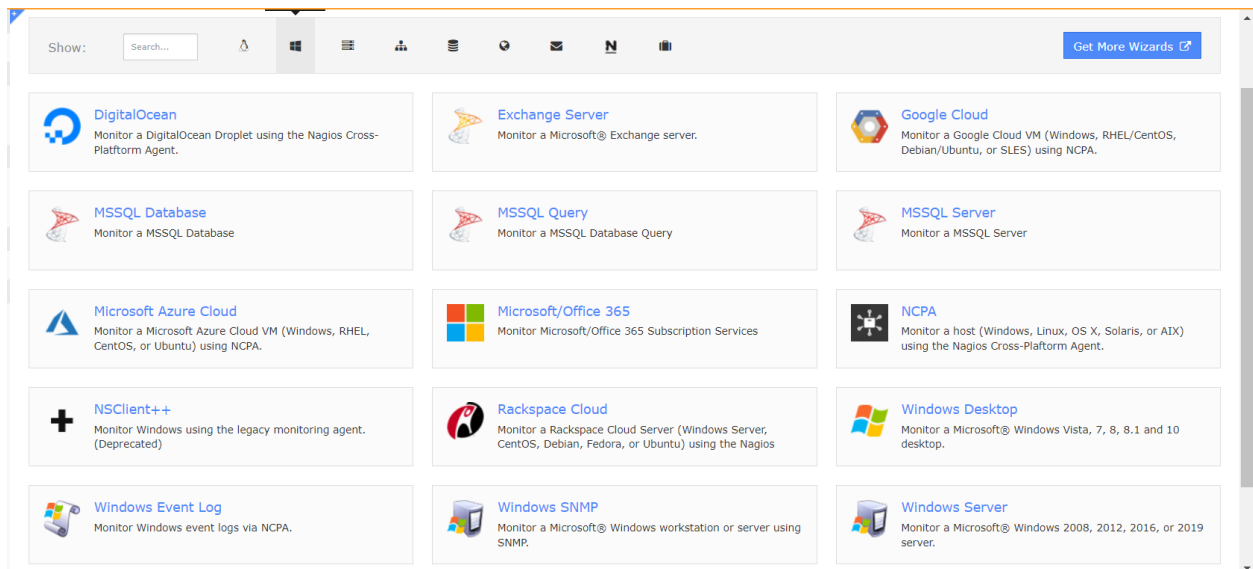


Bước 4: Tạo host trên Nagios XI Server


Vào mục Configure ⇒ Configuration Wizards




Chọn biểu tượng Windows ⇒ Windows SNMP (hoặc có thể search Windows SNMP)



Nhập địa chỉ IP của máy Windows đã kiểm tra ở bước 1. Dịch vụ SNMP trên Windows sử dụng version 2c và port lắng nghe là 161. Tiếp theo ta cần nhập SNMP Community mà ta đã tạo ở bước 3 và nhấn Next.



Configuration Wizard: Windows SNMP - Step 1



Windows Machine Information

IP Address:

The IP address of the Windows machine you'd like to monitor.

Operating System:

Windows 10

▼

SNMP Settings

Specify the settings used to monitor the Windows machine via SNMP.

SNMP Version:

2c

▼

The SNMP protocol version used to communicate with the machine.
You may need to use SNMP v1 if your Windows system language is not English.

SNMP Port:

161

The SNMP port to use, the default is port 161.

SNMP Version Settings

SNMP Community:

public

The SNMP community string required used to query the Windows machine.

< Back

Next >

Ở mục tiếp theo ta có thể tùy chỉnh các mức thông số CPU, RAM, bộ nhớ trống của ổ đĩa mà ta muốn Server sẽ đưa ra cảnh báo

+

Server Metrics

Specify which services you'd like to monitor for the Windows machine.

☒ **Ping**
Monitors the machine with an ICMP "ping". Useful for watching network latency and general uptime.

☒ **CPU**
Monitors the CPU (processor usage) on the machine.

⚠

80

%

!

90

%

☒ **Physical Memory Usage**
Monitors the physical (real) memory usage on the machine.

⚠

80

%

!

90

%

☒ **Virtual Memory Usage**
Monitors the virtual memory usage on the machine.

⚠

5

%

!

10

%

☒ **Disk Usage**
Monitors disk usage on the machine.

The wizard will populate detected drives automatically. To add more drives select a new drive from the dropdown list.

Drive:

C: ▾

⚠

80

%

!

95

%

Drive:

D: ▾

⚠

80

%

!

95

%

Add Row

 |

Delete Row

Ta có thể add các Services cũng như Proccess mà chúng ta muốn Server giám sát.

Services

Specify any services that should be monitored to ensure they're in a running state.
Note: The Windows Service name must match the full name of the service you want to monitor.

The SNMP wizard detected 145 services on 192.168.0.100

Windows Service	Display Name	Scanned Service List
<input type="checkbox"/>		3CX Event Notification Manager
<input type="checkbox"/>		3CX Gateway Service
<input type="checkbox"/>		3CX PhoneSystem 01 AudioProvider
<input type="checkbox"/>		3CX PhoneSystem 01 Call Flow Server
<input type="checkbox"/>		3CX PhoneSystem 01 Configuration Server
<input type="checkbox"/>		3CX PhoneSystem 01 IVR Server
<input type="checkbox"/>		3CX PhoneSystem 01 Management Console
<input type="checkbox"/>		3CX PhoneSystem 01 Queue Manager Server

Add Selected | Select All

Add Row | Delete Row

Processes

Specify any processes that should be monitored to ensure they're running.
Note: Process names are case-sensitive.

The SNMP wizard detected 101 processes on 192.168.0.100

Windows Process	Display Name	Scanned Process List
<input type="checkbox"/>		3CXAudioProvider.exe
<input type="checkbox"/>		3CXCallFlow.exe
<input type="checkbox"/>		3CXGatewayService.exe
<input type="checkbox"/>		3CXIVR.exe
<input type="checkbox"/>		3CXManagementConsole.exe
<input type="checkbox"/>		3CVMediaServer.exe

Tiếp theo Server sẽ cho chúng ta thiết lập khoảng cách giữa các lần mà server sẽ giám sát các host và services cũng như kiểm tra lại trước khi gửi cảnh báo đến người dùng.

Configuration Wizard: Windows SNMP - Step 3

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:

Monitor the host and service(s) every 5 minutes.

When a potential problem is first detected:


Re-check the host and service(s) every 1 minutes up to 5 times before sending a notification.

Back


Next

Finish

Tiếp theo là các cài đặt liên quan đến việc gửi cảnh báo đến admin hay các users và nhấn Finish



Configuration Wizard: Windows SNMP - Step 4



Notification Settings

Define basic parameters that determine how notifications should be sent for the host and service(s).

When a problem is detected:

☐ Don't send any notifications
 ☒ Send a notification immediately
 ☐ Wait minutes before sending a notification

If problems persist:

Send a notification every minutes until the problem is resolved.

Send alert notifications to:

☒ Myself ([Adjust my settings](#))
 ☒ Other individual contacts

Sau khi add host thành công, ta chọn Home → Host Status → và chọn host đã tạo

Notice: This trial copy of Nagios XI will expire in 30 days. [Purchase a License Now](#) or [Enter your license key](#).

Quick View

- Home Dashboard
- Tactical Overview
- Birdseye
- Operations Center
- Operations Screen
- Open Service Problems
- Open Host Problems
- All Service Problems
- All Host Problems
- Network Outages

Details

- Service Status
- Host Status
- Hostgroup Summary
- Hostgroup Overview
- Hostgroup Grid
- Servicegroup Summary
- Servicegroup Overview
- Servicegroup Grid
- BPI
- Metrics

Graphs

- Performance Graphs
- Graph Explorer

Maps

- World Map
- BBmap
- Hypermap
- Minemap

Host Status

All hosts

Host Status Summary

Up	Down	Unreachable	Pending
15	0	0	0
Unhandled	Problems	All	
0	0	2	

Last Updated: 2022-05-20 16:42:19

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
15	0	0	0	3
Unhandled	Problems	All		
0	0	18		

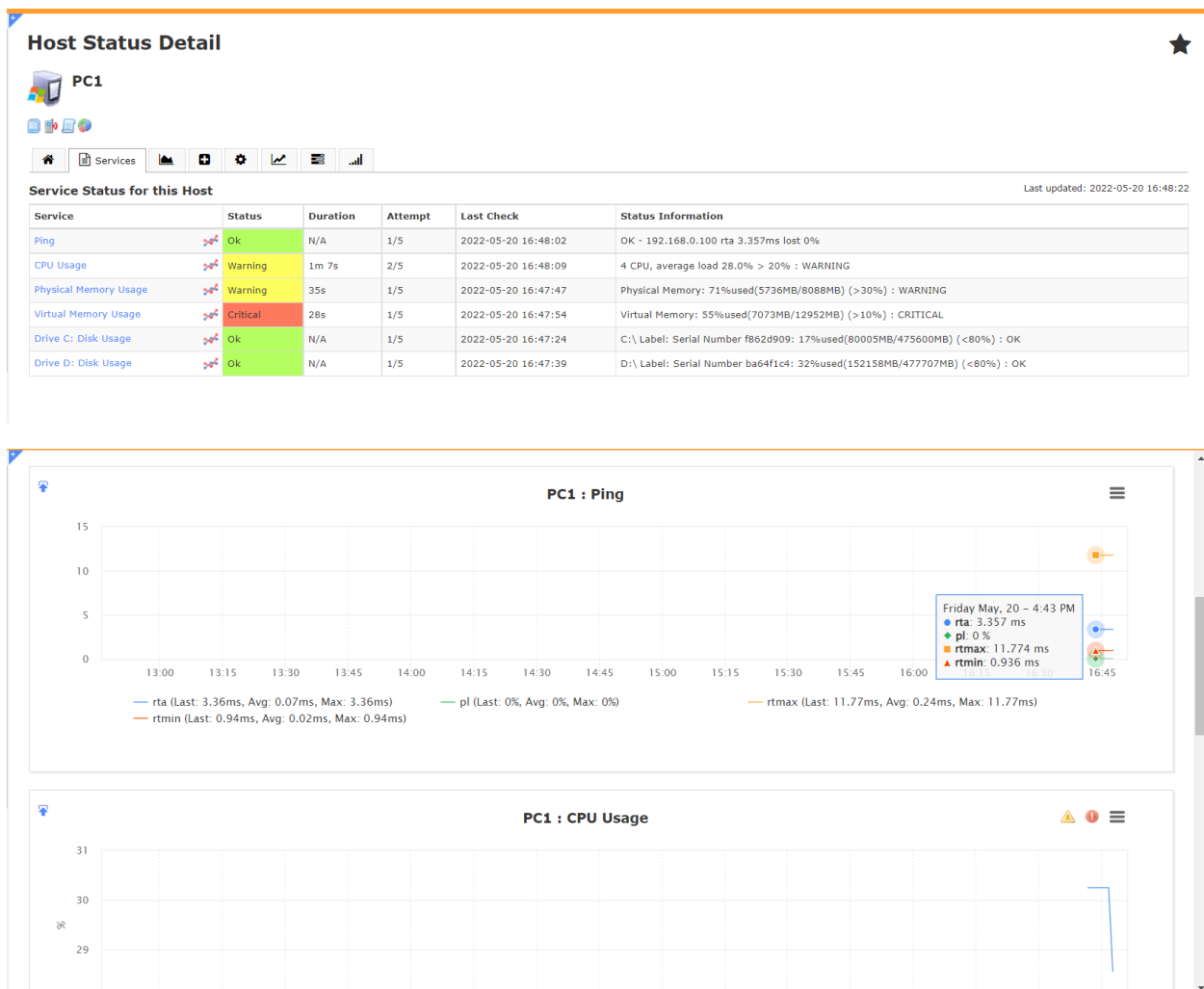
Last Updated: 2022-05-20 16:42:19

Showing 1-2 of 2 total records

Host	Status	Duration	Attempt	Last Check	Status Information
PC1	Up	N/A	1/5	2022-05-20 16:40:25	OK - 192.168.0.100 rta 2.788ms lost 0%
localhost	Up	72d 14h 39m 24s	1/10	2022-05-20 16:38:43	OK - 127.0.0.1 rta 0.020ms lost 0%

Last Updated: 2022-05-20 16:42:19

Ta có thể xem các thông số cũng như mức độ cảnh báo của một host

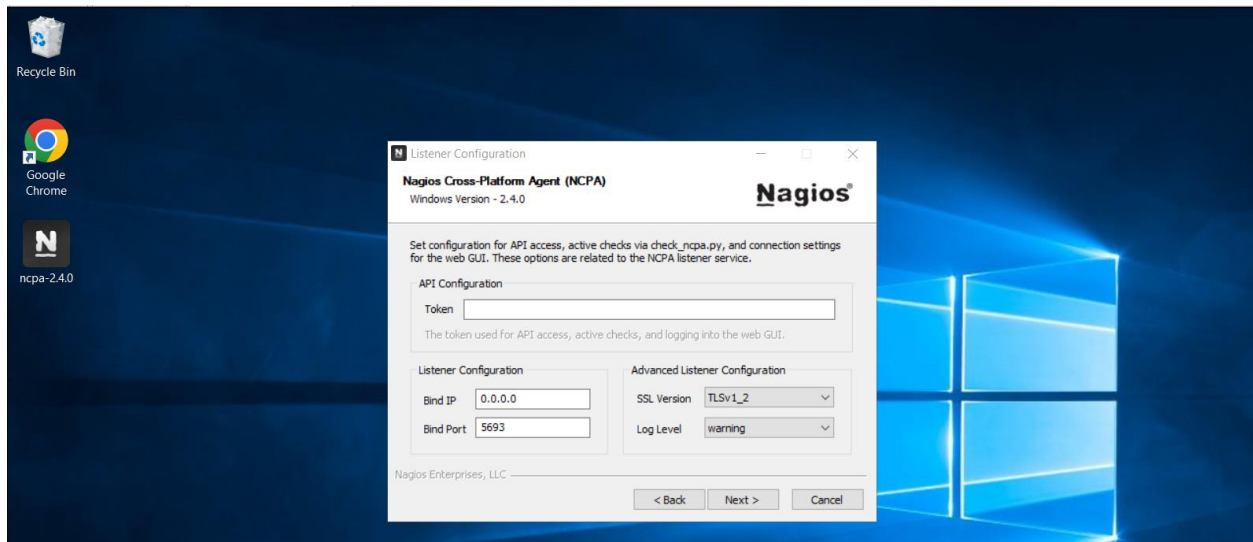


5.3.2 Giám sát Windows Server bằng NCPA

Bước 1: Tải và cài đặt NCPA

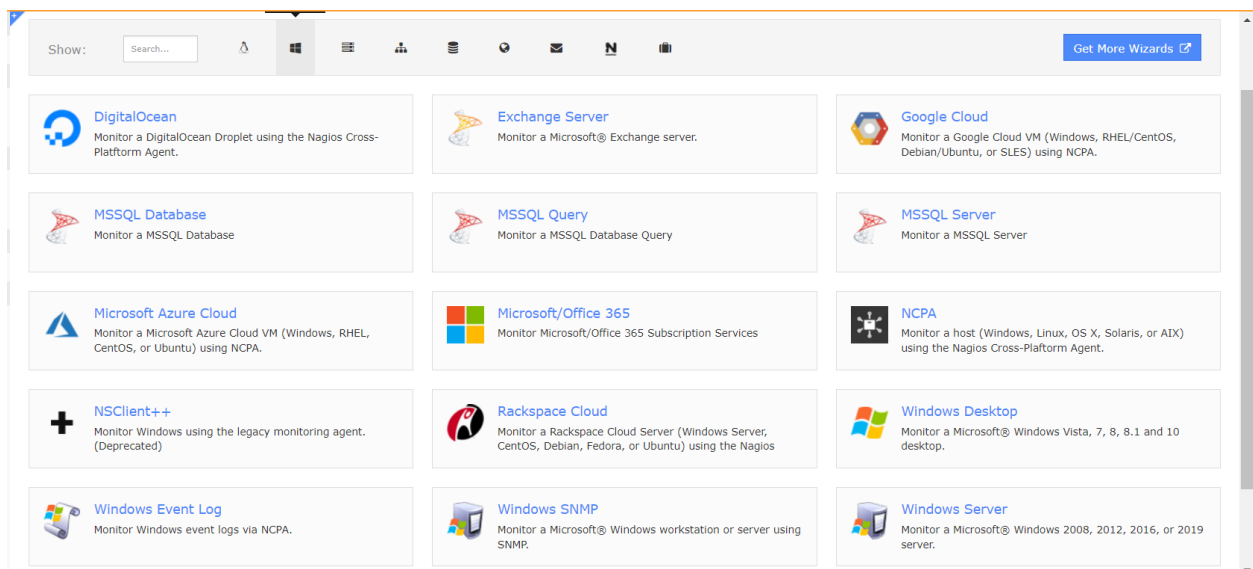
Để có thể tải NCPA ta truy cập link sau: <https://www.nagios.org/ncpa/#downloads>

Ta nhập token tùy ý vào mục token và nhấn next cho đến hết để cài đặt



Bước 2: Add Windows Server trên Nagios XI Server

Vào mục Configure ⇒ Configuration Wizards ⇒ Chọn biểu tượng Windows ⇒ Windows Server (hoặc có thể search Windows Server).



Tiếp theo ta nhập địa chỉ IP của Windows Server và token mà chúng ta đã tạo ở bước 1 và nhấn next.

Cũng như add host bằng SNMP, ta có thể tùy chỉnh các mức số liệu mà Server sẽ đưa ra cảnh báo cũng như thêm các Services hay process trên Windows Server vào việc giám sát (Các bước tiếp theo tương tự như cách add host ở trên).

System Metrics

Specify the metrics you'd like to monitor on the NCPA Agent.

☒ CPU Usage
 Check the CPU usage of the system.

20

%

40

%

☒ Show average CPU usage instead of per cpu core

Current CPU Usage

0%

☒ User Count
 Check the number of users currently logged into the system.

2

#

4

#

Current User Count

1

Memory Metrics

Default units to use for memory metric output: Gi

☒ Main Memory Usage
 Monitor memory usage as percentage of memory used.

50

%

80

%

☒ Swap Usage
 Monitor the percentage of allocated swap used.

5

%

10

%

Current Memory Usage

33.9%

Current Swap Usage

23.3%

Disk Metrics

Sau khi add host thành công, ta có thể kiểm tra tình trạng của Windows Server thông qua RAM, CPU cũng như có thể phân tích các thông số dựa trên biểu đồ mà Nagios cung cấp

Host Status Detail

★

Windows Server

Home

Services

Hosts

Settings

Graphs

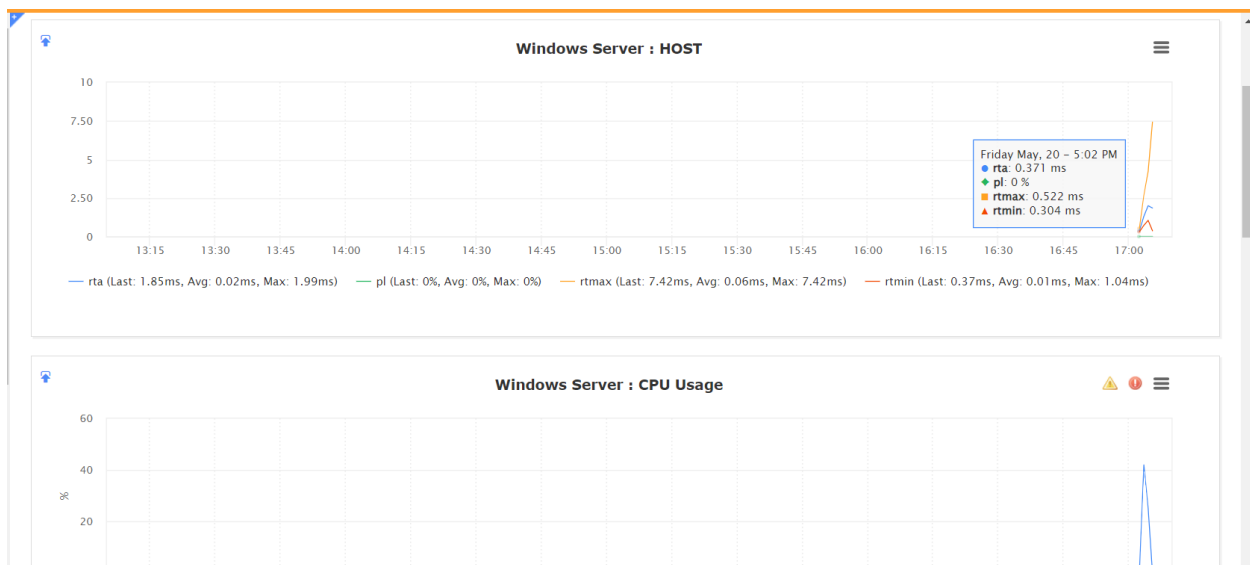
Logs

Alerts

Service Status for this Host

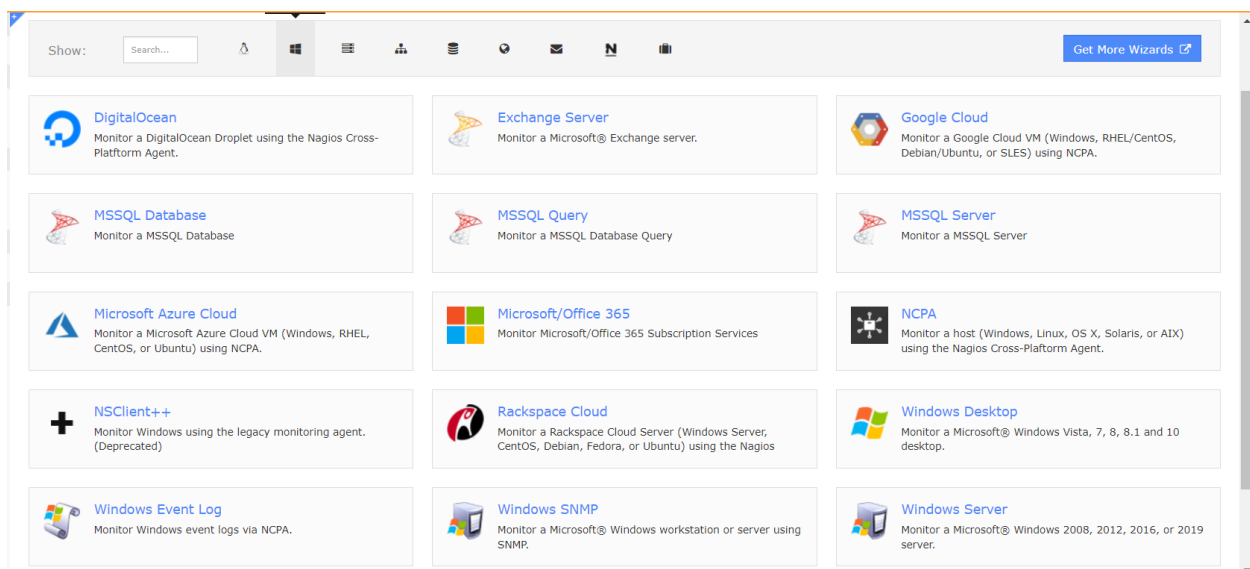
Last updated: 2022-05-20 17:07:23

Service	Status	Duration	Attempt	Last Check	Status Information
CPU Usage	Ok	2m 3s	1/5	2022-05-20 17:07:18	OK: Percent was 0.00 %
User Count	Ok	4m 22s	1/5	2022-05-20 17:07:00	OK: Count was 1 users
Memory Usage	Ok	4m 29s	1/5	2022-05-20 17:06:50	OK: Memory usage was 34.00 % (Available: 2.64 GiB, Total: 4.00 GiB, Free: 2.64 GiB, Used: 1.36 GiB)
Swap Usage	Critical	29s	5/5	2022-05-20 17:06:54	CRITICAL: Swap usage was 23.90 % (Total: 5.37 GiB, Used: 1.28 GiB, Free: 4.09 GiB)
Disk Usage on D:/	Critical	43s	5/5	2022-05-20 17:06:40	CRITICAL: Used disk space was 100.00 % (Used: 4.93 GiB, Free: 0.00 GiB, Total: 4.93 GiB)
Disk Usage on C:/	Ok	4m 43s	1/5	2022-05-20 17:06:37	OK: Used disk space was 58.20 % (Used: 11.29 GiB, Free: 8.11 GiB, Total: 19.40 GiB)
Ethernet0 2 Bandwidth - Outbound	Ok	4m 33s	1/5	2022-05-20 17:06:47	OK: Bytes_sent was 0.00 MB/s
Ethernet0 2 Bandwidth - Inbound	Ok	4m 36s	1/5	2022-05-20 17:06:43	OK: Bytes_recv was 0.00 MB/s



5.3.3 Giám sát Windows bằng NSClient++

Vào mục Configure ⇒ Configuration Wizards ⇒ Chọn biểu tượng Windows ⇒ NSClient++ (hoặc có thể search NSClient++).



Nhập địa chỉ IP của máy Windows và nhấn next.

Configuration Wizard: NSClient++ - Step 1

Host Information

IP Address:

192.168.0.130

The IP address of the Windows system you'd like to monitor.

< Back

Next >

Ta cần chọn phiên bản Agent phù hợp với máy của mình và tải xuống

Configuration Wizard: NSClient++ - Step 2

Host Details

IP Address:

192.168.0.130

Host Name:

PC2

The name you'd like to have associated with this Windows system.

NSClient++ Agent


You'll need to install an agent on the Windows system in order to monitor it. For security purposes, it is recommended to use a password with the agent.


This config wizard is **deprecated**. We recommend using the [Windows Server](#) or [Windows Desktop](#) configuration wizard instead.

32-Bit Agent

64-Bit Agent

Agent Download:

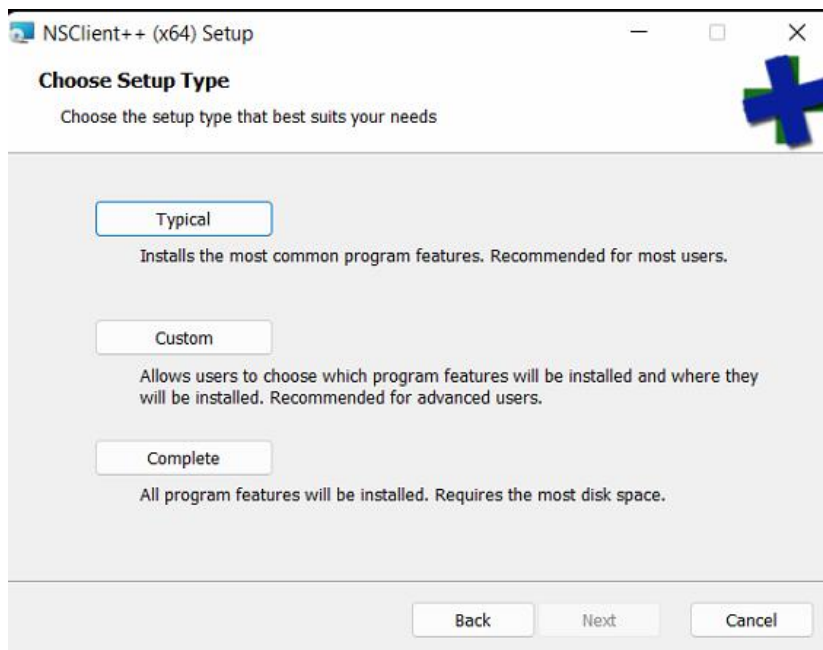
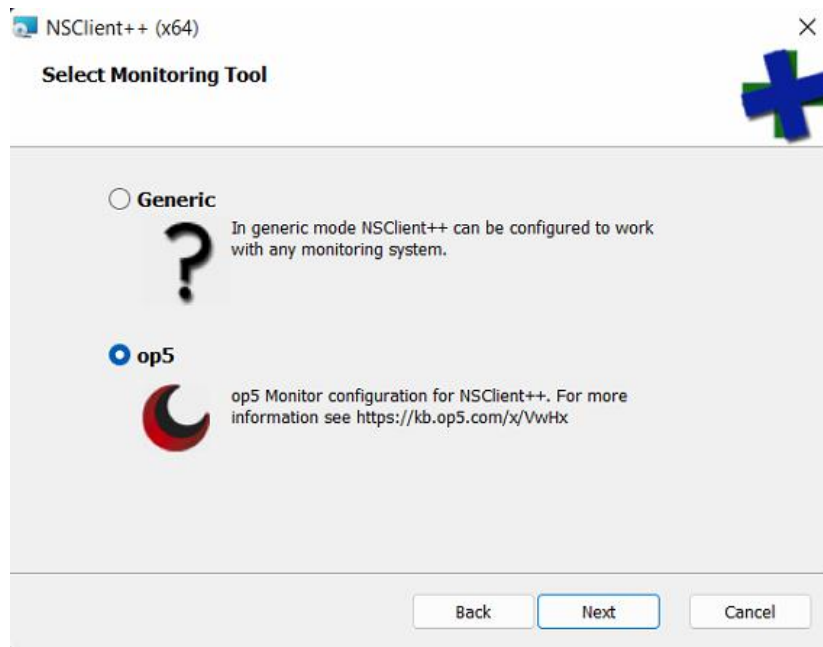
 [Download v0.4.4 \(32bit\)](#)

 [Download v0.4.4 \(64bit\)](#)

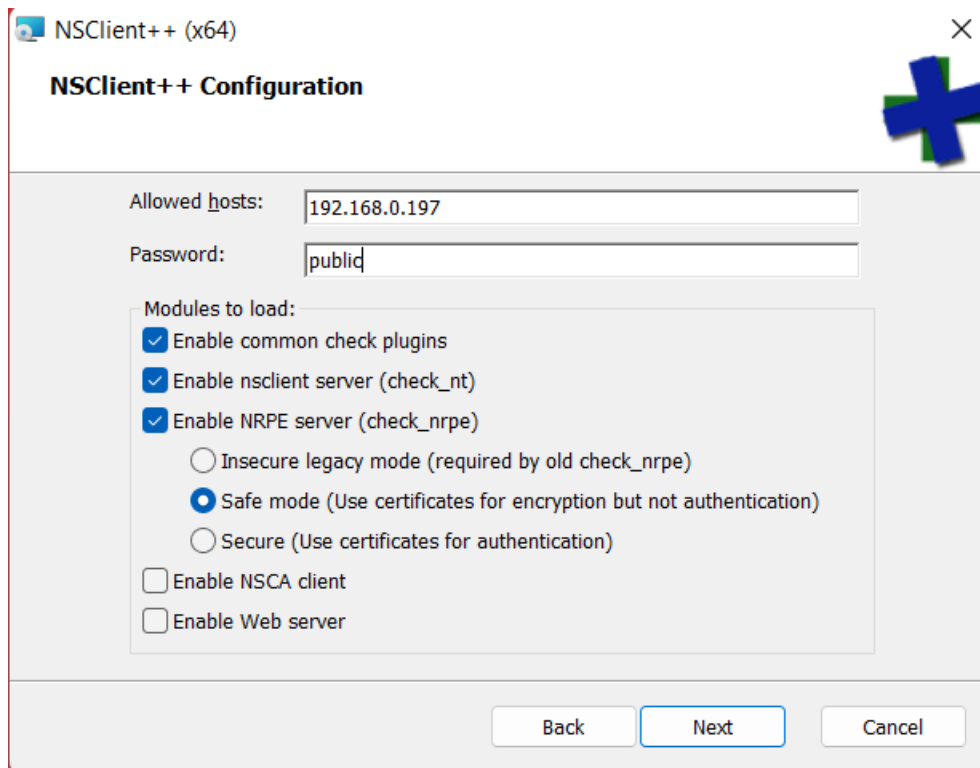
Agent Password:

Valid characters include: **a-zA-Z0-9**.\!:_-@

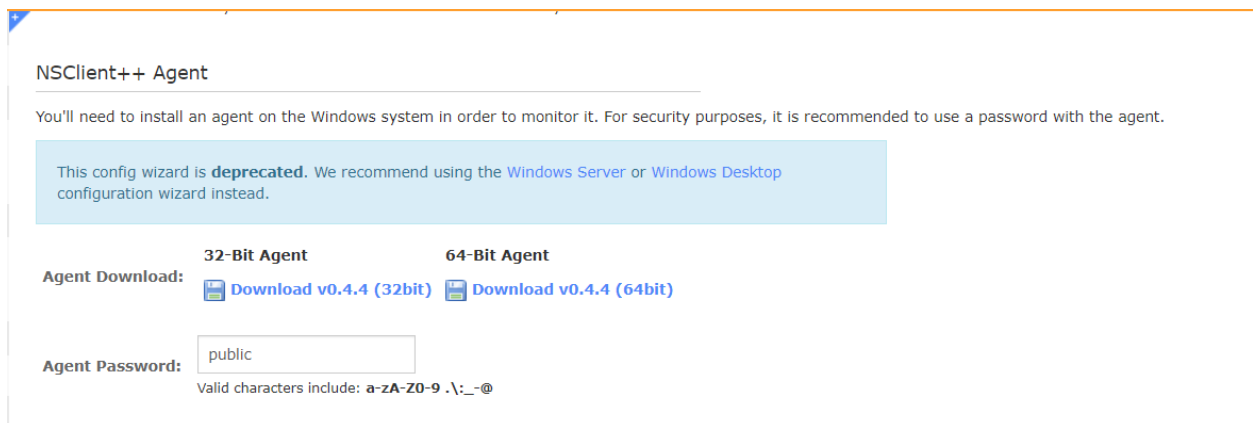
Tiếp theo ta cần cài đặt NSClient++, ở phần cài đặt ta chọn mục Generic → Typical



Ở mục Allowed hosts, ta nhập địa chỉ IP của Nagios Server và nhập password, sau đó nhấn next.



Sau khi cài đặt xong NSClient++, ta quay trở lại Nagios Server và nhập Agent password theo password mà ta vừa đặt trong phần cài đặt NSClient++.



Tiếp theo tương tự các cách add host trên, ta có thể tùy chỉnh các thông số để Server có thể đưa ra cảnh báo cũng như thêm các Services cũng như Process để Server có thể giám sát.

Specify which services you'd like to monitor for the system.

- ☒ **Ping**
Monitors the server with an ICMP ping. Useful for watching network latency and general uptime.
- ☒ **CPU**
Monitors the CPU (processor usage) on the server.
⚠️ 80 % ⓘ 90 %
- ☒ **Memory Usage**
Monitors the memory usage on the server.
⚠️ 80 % ⓘ 90 %
- ☒ **Uptime**
Monitors the uptime on the server.
- ☒ **Disk Usage**
Monitors disk usage on the server.
Drive: C: ⚠️ 80 % ⓘ 95 %
Drive: ⚠️ 80 % ⓘ 95 %
Drive: ⚠️ 80 % ⓘ 95 %
Drive: ⚠️ 80 % ⓘ 95 %
Drive: ⚠️ 80 % ⓘ 95 %

[Add Row](#) | [Delete Row](#)

5.3.4 Giám sát Router bằng giao thức SNMP

Bước 1: Cấu hình dịch vụ SNMP trên Router

Để có thể giám sát router thông qua giao thức SNMP, ta cần phải cấu hình dịch vụ SNMP trên Router bằng các câu lệnh sau:

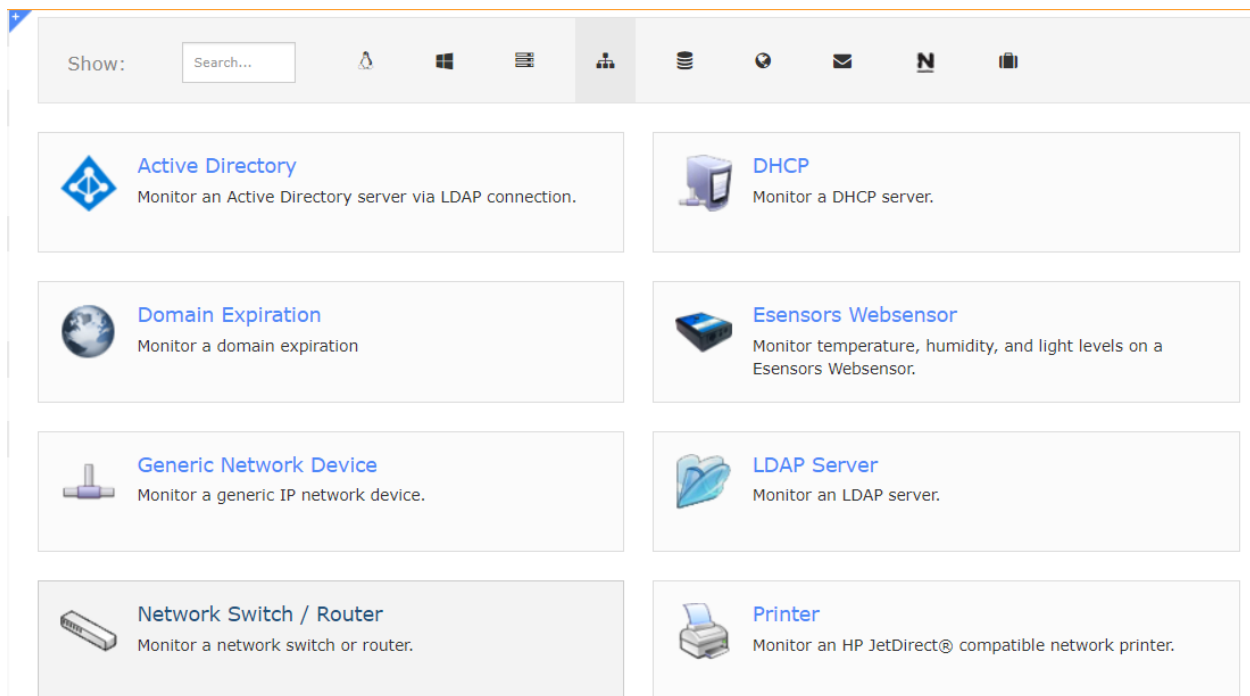
- Khai báo chuỗi SNMP Community
snmp-server community public ro
- Bật dịch vụ SNMP
snmp-server enable traps snmp
- Khai báo thông tin về Router (mô tả tùy ý về contact, location)
snmp-server contact "Nhom15"
snmp-server location "Nhom15"

Lưu ý: “public” là chuỗi Community

```
R1(config)#
R1(config)#snmp-server community public ro
R1(config)#snmp-server enable traps snmp
R1(config)#snmp-server contact "Nhom15"
R1(config)#snmp-server location "Nhom15"
R1(config)#
```

Bước 2: Tạo host Router trên Nagios Server

Vào mục Configure ⇒ Configuration Wizards ⇒ Chọn biểu tượng Network ⇒ Network Switch/Router







Tiếp theo ta nhập địa chỉ IP của router



Ngoài ra ta có thể tùy chỉnh các mức độ về Input/Output Rate để Nagios có thể đưa ra các cảnh báo và nhấn next.

Default Values

 Input Rate:	<input type="text" value="50"/>	%	 Input Rate:	<input type="text" value="80"/>	%
 Output Rate:	<input type="text" value="50"/>	%	 Output Rate:	<input type="text" value="80"/>	%
Default Port Speed:	<input type="text" value="100"/>	Mbps			

[< Back](#)[Next >](#)

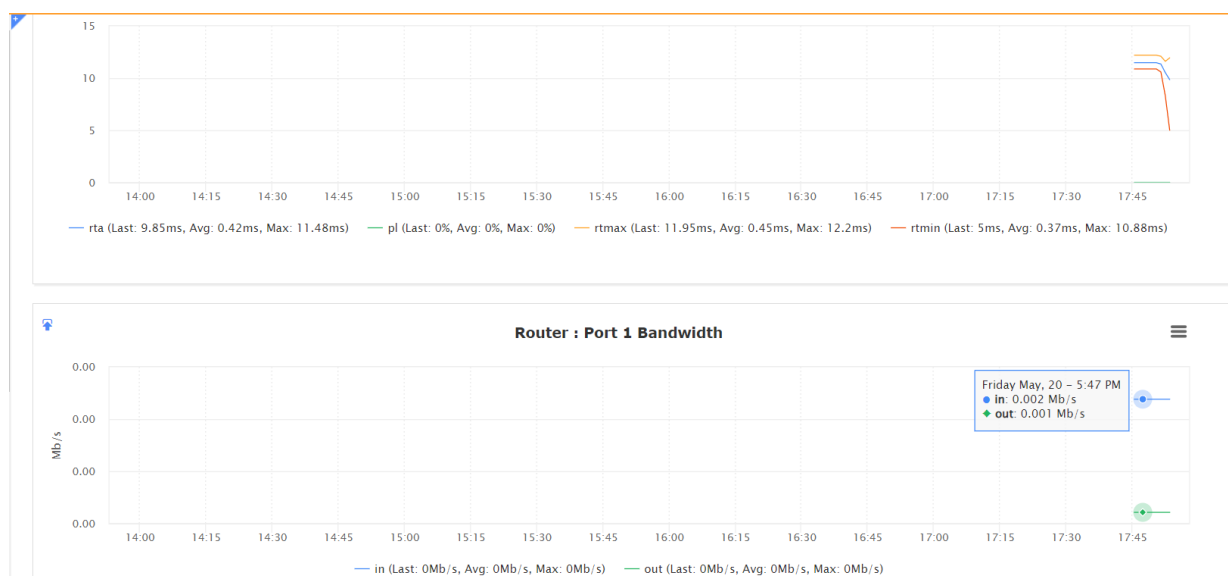
Tiếp theo, ta có thể tùy chỉnh băng thông Rate In/Out của các port để Server có thể cảnh báo khi vượt qua các mức mà ta tùy chỉnh.

<

Các bước sau tương tự các cách tạo host ở trên.

Sau khi tạo host thành công, ta có thể kiểm tra tình trạng các port cũng như băng thông của các port trên router.

Service Status for this Host						Last updated: 2022-05-20 17:52:43
Service	Status	Duration	Attempt	Last Check	Status Information	
Ping	Ok	N/A	1/5	2022-05-20 17:51:51	OK - 192.168.0.124 rta 11.478ms lost 0%	
Port 1 Bandwidth	Ok	N/A	1/5	2022-05-20 17:52:01	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 1 Status	Ok	N/A	1/5	2022-05-20 17:52:09	OK: Interface FastEthernet0/0 (index 1) is up.	
Port 2 Bandwidth	Ok	N/A	1/5	2022-05-20 17:52:26	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 2 Status	Warning	16s	1/5	2022-05-20 17:52:27	WARNING: Interface GigabitEthernet1/0 (index 2) is administratively down.	
Port 3 Bandwidth	Ok	N/A	1/5	2022-05-20 17:52:28	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 3 Status	Warning	1m 0s	1/5	2022-05-20 17:51:43	WARNING: Interface GigabitEthernet2/0 (index 3) is administratively down.	
Port 4 Bandwidth	Ok	N/A	1/5	2022-05-20 17:51:54	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 4 Status	Warning	40s	1/5	2022-05-20 17:52:03	WARNING: Interface GigabitEthernet3/0 (index 4) is administratively down.	
Port 5 Bandwidth	Ok	N/A	1/5	2022-05-20 17:52:11	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 5 Status	Warning	24s	1/5	2022-05-20 17:52:19	WARNING: Interface FastEthernet4/0 (index 5) is administratively down.	
Port 6 Bandwidth	Ok	N/A	1/5	2022-05-20 17:52:30	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 6 Status	Warning	12s	1/5	2022-05-20 17:52:31	WARNING: Interface FastEthernet4/1 (index 6) is administratively down.	
Port 7 Bandwidth	Ok	N/A	1/5	2022-05-20 17:52:32	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 7 Status	Warning	8s	1/5	2022-05-20 17:52:35	WARNING: Interface FastEthernet5/0 (index 7) is administratively down.	
Port 8 Bandwidth	Ok	N/A	1/5	2022-05-20 17:52:34	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 8 Status	Warning	7s	1/5	2022-05-20 17:52:36	WARNING: Interface FastEthernet5/1 (index 8) is administratively down.	
Port 9 Bandwidth	Ok	N/A	1/5	2022-05-20 17:51:45	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 9 Status	Warning	47s	1/5	2022-05-20 17:51:56	WARNING: Interface FastEthernet6/0 (index 9) is administratively down.	
Port 10 Bandwidth	Ok	N/A	1/5	2022-05-20 17:52:16	OK - Current BW in: 0Mbps Out: 0Mbps	
Port 10 Status	Warning	21s	1/5	2022-05-20 17:52:22	WARNING: Interface FastEthernet6/1 (index 10) is administratively down.	



5.4 Cài đặt Nagios Network Analyzer (Nagios NA)

5.4.1 Cài đặt Nagios NA

Để có thể cài đặt Nagios NA ta truy cập đường link sau đây:

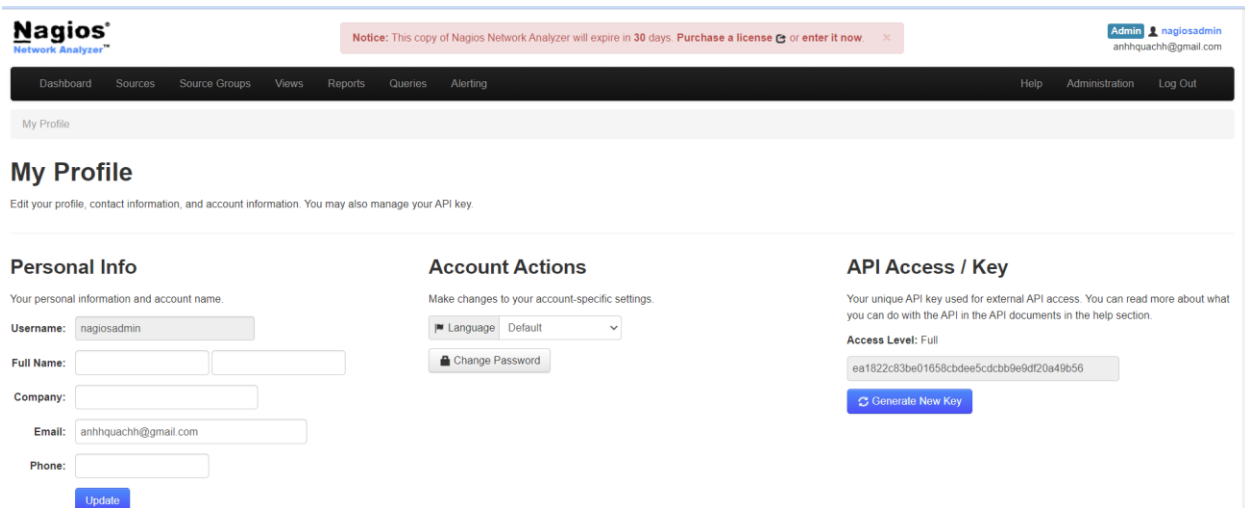
<https://www.nagios.com/downloads/nagios-network-analyzer/>

Các bước cài đặt tương tự Nagios XI (mục 5.2)

5.4.2 Kết nối Nagios NA và Nagios XI

Bước 1: Kiểm tra API Access/ Key của admin trên Nagios NA

Click vào nagiosadmin ở góc trên bên phải và copy API Access/Key



Nagios
Network Analyzer™

Notice: This copy of Nagios Network Analyzer will expire in 30 days. [Purchase a license](#) or [enter it now](#)

Admin 1 nagiosadmin
anhquachh@gmail.com

Dashboard Sources Source Groups Views Reports Queries Alerting Help Administration Log Out

My Profile

My Profile

Edit your profile, contact information, and account information. You may also manage your API key.

Personal Info

Your personal information and account name.

Username:

Full Name:

Company:

Email:

Phone:

[Update](#)

Account Actions

Make changes to your account-specific settings.

Language:

[Change Password](#)

API Access / Key

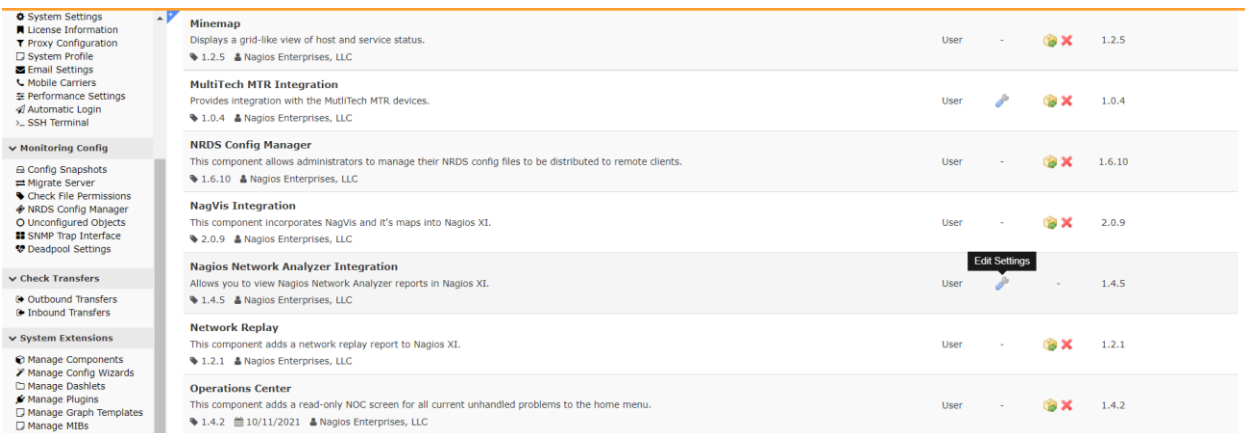
Your unique API key used for external API access. You can read more about what you can do with the API in the API documents in the help section.

Access Level: Full

[Generate New Key](#)

Bước 2: Kết nối Nagios NA với Nagios XI

Quay về Nagios XI, chọn Admin ⇒ Manage Component ⇒ Nagios Network Analyzer Integration ⇒ Edit Settings ⇒ Add a Server



System Settings	Minemap Displays a grid-like view of host and service status. 1.2.5 Nagios Enterprises, LLC	User	-		1.2.5
License Information	MultiTech MTR Integration Provides integration with the MultiTech MTR devices. 1.0.4 Nagios Enterprises, LLC	User			1.0.4
Proxy Configuration	NRDS Config Manager This component allows administrators to manage their NRDS config files to be distributed to remote clients. 1.6.10 Nagios Enterprises, LLC	User	-		1.6.10
System Profile	NagVis Integration This component incorporates NagVis and it's maps into Nagios XI. 2.0.9 Nagios Enterprises, LLC	User	-		2.0.9
Email Settings	Nagios Network Analyzer Integration Allows you to view Nagios Network Analyzer reports in Nagios XI. 1.4.5 Nagios Enterprises, LLC	User		Edit Settings	1.4.5
Mobile Carriers	Network Replay This component adds a network replay report to Nagios XI. 1.2.1 Nagios Enterprises, LLC	User	-		1.2.1
Performance Settings	Operations Center This component adds a read-only NOC screen for all current unhandled problems to the home menu. 1.4.2 10/11/2021 Nagios Enterprises, LLC	User	-		1.4.2
Automatic Login					
SSH Terminal					

Điền tên của Nagios NA, địa chỉ IP của Nagios NA và API Key đã copy trước đó và nhấn Apply Settings.

Nagios Network Analyzer Integration

?

★

Component Settings

These are all the general settings for this component.

☐ Disable Host/Service Tabs from being shown

Nagios Network Analyzer Servers

Specify the addresses and a users API Key for each of the Nagios Network Analyzer servers you'd like to see from inside Nagios XI.

[Add a Server](#)

Nagios Network Analyzer Servers				
Name: NagiosNA	IP Address / Hostname: 192.168.0.196	API Key: ea1822c83be01658cbdee5cdcb9e9	<input type="checkbox"/> Use SSL <input type="checkbox"/> Allow invalid certificate	Lookback period @: 4

Apply Settings

Cancel

5.5 Nagios NA phân tích dữ liệu từ Router

Bước 1: Cấu hình Netflow data trên Router

Để Nagios NA có thể phân tích các flow data đi qua Router, ta cần cấu hình Netflow trên Router bằng các câu lệnh sau:

#int fa0/0

#ip route-cache flow

#ip flow-export destination 192.168.0.196 9912

#ip flow-export version 9

Lưu ý: 192.168.0.196 là địa chỉ IP của Nagios NA và 9912 là port mà router sử dụng là 9912.

```
R1(config-if)#
R1(config-if)#int fa0/0
R1(config-if)#ip route-cache flow
R1(config-if)#ip flow-export des 192.168.0.196 9912
R1(config)#ip flow-export version 9
R1(config)#
```

Bước 2: Create Source trên Nagios NA

Trên Nagios NA, Sources ⇒ Create Source

DashboardSourcesSource GroupsViewsReportsQueriesAlertingHelpAdministration

Sources / Create Source

Create Source

When adding a new source, make sure you set up the source to send flow data to your NNA installation IP address at the port you specify below to receive data.

Source Name*:

Must be unique. Name of the flow data collector. Used in back-end file system. Use a nice name that is easily associated with the flow data sending device.

Sender IP Address(es):

Optional. Use this to internally show what IP address(es) of switches, routers, or servers are sending to this source.

Listening Port*:

Must be unique. Port that the flow data is received on for this source. Multiple switches, routers, and servers can send to one port.

Incoming Flow Type:

NetFlow

Use NetFlow if you're using a device that supports NetFlow, JFlow, IPFIX, etc.

Raw Data Lifetime:

24

Hours

The length of time you want **granular flow data** to be stored on your server, recommended 24hr period saves disk space. [More info.](#)

☐ Disable abnormal behavior checks (removes from front page)

[Advanced Settings](#)

Ở mục Sender IP Address, ta điền các địa chỉ IP mà router sẽ gửi dữ liệu đến các địa chỉ này, listening port là port mà ta đã cấu hình trên Router ở bước 1 (port 9912) và nhấn creat source.

Source Name*:

Router

Must be unique. Name of the flow data collector. Used in back-end file system. Use a nice name that is easily associated with the flow data sending device.

Sender IP Address(es):

192.168.0.100
192.168.0.130

Optional. Use this to internally show what IP address(es) of switches, routers, or servers are sending to this source.

Listening Port*:

9912

Must be unique. Port that the flow data is received on for this source. Multiple switches, routers, and servers can send to one port.

Incoming Flow Type:

NetFlow

Use NetFlow if you're using a device that supports NetFlow, JFlow, IPFIX, etc.

Raw Data Lifetime:

24

Hours

The length of time you want **granular flow data** to be stored on your server, recommended 24hr period saves disk space. [More info.](#)

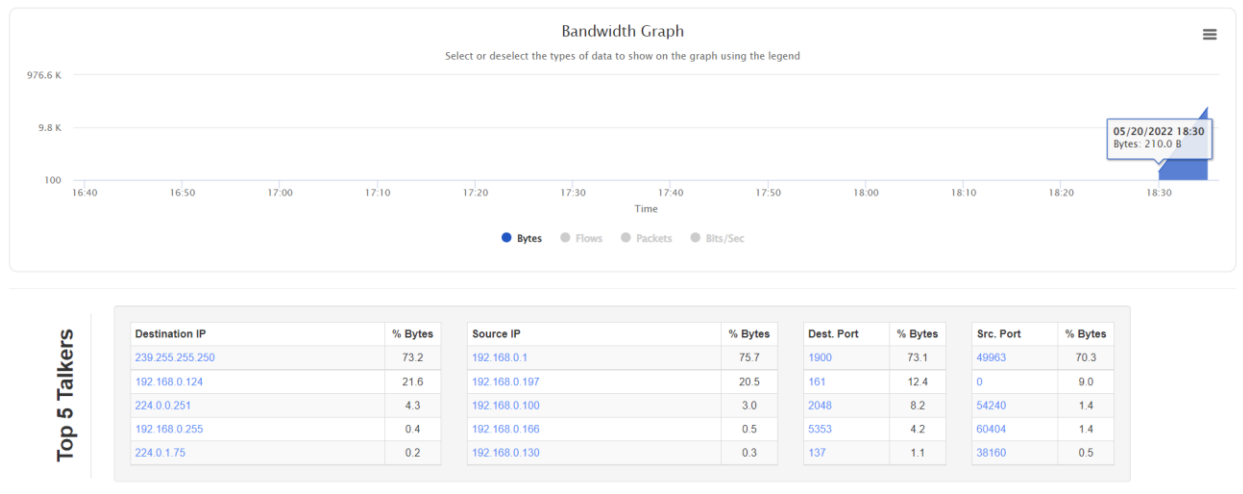
☐ Disable abnormal behavior checks (removes from front page)

[Advanced Settings](#)

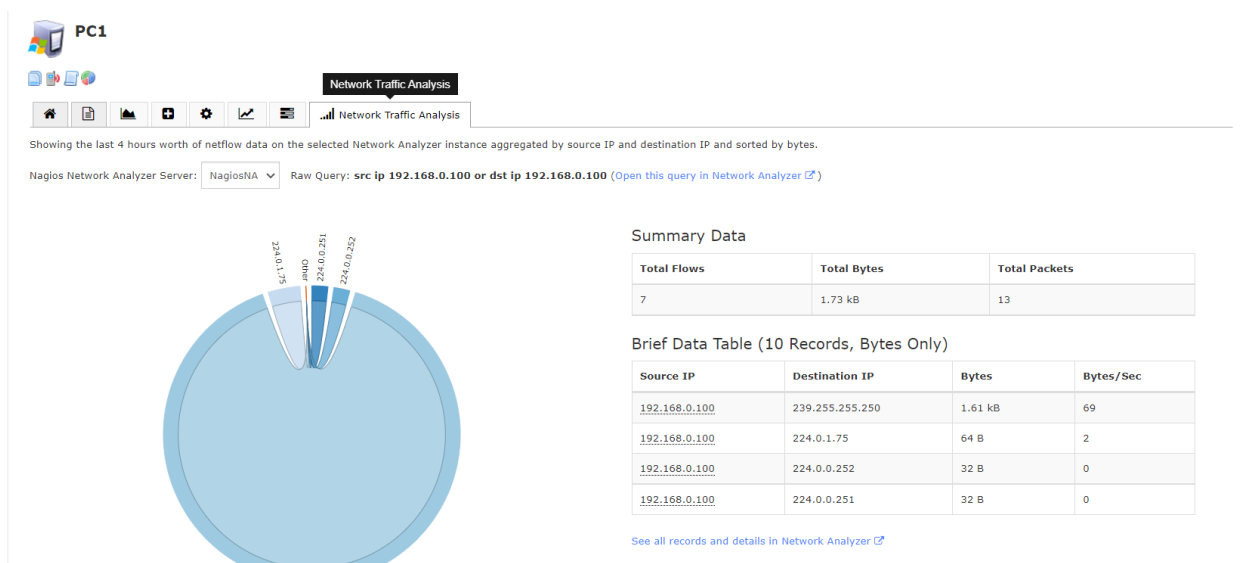
Create Source

Cancel

Sau khi create source thành công, mất khoảng 5 đến 15 để Server có thể hiển thị các thông tin cần thiết cũng như các biểu đồ.



Ngoài ra, trên Nagios XI sau khi đã kết nối với Nagios NA ta cũng có thể xem các phân tích về các host mà ta đã add.



CHƯƠNG 6: TÀI LIỆU THAM KHẢO

- [1] Network traffic monitoring: NagiOS.
- [2] SNMPtoantap_DiepThanhNguyen.
- [3] <https://assets.nagios.com/downloads/nagiosxi/guides/user/>.
- [4] <https://assets.nagios.com/downloads/nagios-network-analyzer/guides/nna-ag/>.
- [5] <https://www.nagios.com/resources/nagios-xi/>.
- [6] <https://www.nagios.com/resources/network-analyzer/>.