

Học viện Công nghệ Bưu chính Viễn thông
Cơ Sở TP. HCM



BÁO CÁO LẦN I

Môn: An Ninh Mạng

Giảng viên: Trần Thị Dung

Nhóm 10

Thành viên nhóm:

STT	Họ và tên	Mã sinh viên	Lớp	
1	Trần Nguyên Thiên Trí	N18DCAT094	D18CQAT02-N	Nhóm Trưởng
2	Lê Hoàng Anh	N18DCAT004	D18CQAT02-N	
3	Phạm Hoàng Quý	N18DCAT064	D18CQAT02-N	
4	Nguyễn Gia Liêm	N18DCAT038	D18CQAT02-N	
5	Nguyễn Đức Chính	N18DCAT010	D18CQAT02-N	

LỜI MỞ ĐẦU

Ngày nay, tốc độ phát triển CNTT (Công nghệ thông tin) phát triển không ngừng đã giúp cho các doanh nghiệp ứng dụng xây dựng được các cơ sở hạ tầng phục vụ cho nhu cầu sản xuất kinh tế và các lĩnh vực khác của mình. Bởi vậy, khi đi đôi với sự phát triển đó cũng có nhiều rủi ro có thể xảy ra khiến các doanh nghiệp trắng tay nếu không biết kiểm soát và phòng ngừa các rủi ro đó như : mất an toàn về thông tin,... Đó là lúc họ cần phương pháp giám sát, kiểm tra và cảnh báo khi có cơ sở hạ tầng của họ có vấn đề.

Họ cần chọn một phần mềm hay một công cụ có thể đáp ứng những yêu cầu mà họ đề ra, đồng thời có thể linh hoạt trong việc thêm hoặc bớt thiết bị dịch vụ cần giám sát.

Doanh nghiệp lớn họ có thể mua các phần mềm giám sát đáp ứng những yêu cầu này nhưng đối với doanh nghiệp nhỏ họ đôi khi khó khăn trong việc mua những phần mềm đó, cho nên họ đã đưa ra giải pháp là sử dụng các phần mềm giám sát mã nguồn mở chạy trên hệ điều hành mã nguồn mở. Với những phần mềm này, doanh nghiệp nhỏ sẽ dễ dàng cấu hình để các chương trình thực hiện những yêu cầu mà họ cần.

Ngày nay, Doanh nghiệp nhỏ có xu hướng sử dụng các hệ điều hành mở như CentOS, unbutu,...

Đang phát triển mạnh mẽ và đã thể hiện được ưu thế so với việc sử dụng các phần mềm có trả phí. Phần mềm nguồn mở được sử dụng trên hệ điều hành này mang lại nhiều lợi ích cho người sử dụng, trong đó Nagios là một trong số chúng.

MỤC LỤC

I.	BẢNG PHÂN CÔNG VIỆC	1
II.	CƠ SỞ LÝ THUYẾT	1
1.	TỔNG QUAN VỀ HỆ THỐNG GIÁM SÁT	1
1.1.	Những yếu tố trong giám sát hệ thống	1
1.2.	Các công cụ giám sát dựa trên mã nguồn mở.....	2
2.	TỔNG QUAN VỀ NAGIOS.....	2
2.1.	Khái niệm về Nagios	2
2.2.	Chức năng của Nagios.....	3
2.3.	Đặc điểm của Nagios.....	5
2.4.	Mô hình triển khai Nagios	6
2.5.	Kiến trúc và tổ chức hoạt động	7
2.6.	Khả năng giám sát thiết bị	8
2.7.	Các Agent của Nagios	9
III.	CÀI ĐẶT NAGIOS	10
1.	Cài đặt nagios vào Virtualbox.....	10
2.	Thêm các host vào nagios để thực hiện giám sát	12
2.1.	Windows host:	12
2.2.	Linux host:	12
2.3.	Cấu hình giám sát dịch vụ Web	14
2.4.	Giám sát dịch vụ cơ sở dữ liệu Mysql.....	20

I. BẢNG PHÂN CÔNG VIỆC

Họ tên	MSSV	Video
Trần Nguyên Thiên Trí	N18DCAT094	Giám sát dịch vụ cơ sở dữ liệu SQL
Phạm Hoàng Quý	N18DCAT064	Giám sát window
Nguyễn Đức Chính	N18DCAT010	Giám sát web service
Lê Hoàng Anh	N18DCAT004	Tìm hiểu về Nagios, cài đặt và setup cho Nagios cho máy.
Nguyễn Gia Liêm	N18DCAT038	Giám sát Linux

II. CƠ SỞ LÝ THUYẾT

1. TỔNG QUAN VỀ HỆ THỐNG GIÁM SÁT

1.1. Những yếu tố trong giám sát hệ thống

- Giám sát mạng là gì?

Giám sát nôm na là việc chúng ta theo dõi liên tục một đối tượng nào đó 24/7.

⇒ Giám sát mạng là chúng ta theo dõi liên tục một hệ thống (thiết bị hoặc chương trình) hoặc các dịch vụ trong hệ thống mạng.

- Tại sao lại cần giám sát? Giám sát những gì?

Đối với hệ thống mạng doanh nghiệp là vô cùng quan trọng vì chúng ta không biết được rằng trong 1 giây doanh nghiệp có thể kiếm được rất nhiều tiền nếu trong quá trình đó các attacker tấn công thì sẽ gây thiệt hại vô cùng lớn cho công ty doanh nghiệp nên việc giám sát quan trọng nhất là nắm được những thông tin chính xác nhất vào mọi thời điểm (từng giây, từng phút).

Những thông tin cần nắm bắt khi giám sát là :

- ❖ Tính sẵn sàng của thiết bị (Router, Switch, Server,...): những thiết bị giữ cho mạng hoạt động.
- ❖ Các dịch vụ trong hệ thống (DNS, FTP, HTTP,...): những dịch vụ này đóng vai trò quan trọng trong một công ty, tổ chức, nếu các dịch vụ này không được đảm bảo hoạt động bình thường và liên tục, nó sẽ ảnh hưởng nghiêm trọng đến công ty, tổ chức đó.
- ❖ Tài nguyên hệ thống: Các ứng dụng đều đòi hỏi tài nguyên hệ thống, việc giám sát tài nguyên sẽ đảm bảo cho chúng ta có những can thiệp kịp thời, tránh ảnh hưởng đến hệ thống.

- ❖ Lưu lượng trong mạng: nhằm đưa ra những giải pháp, ngăn ngừa hiện tượng quá tải trong mạng.
- ❖ Các chức năng về bảo mật: nhằm đảm bảo an ninh trong hệ thống
- ❖ Nhiệt độ, thông tin về máy chủ, máy in: giúp tránh những hư hỏng xảy ra.
- ❖ Tạo file log: thu được những thông tin về những thay đổi trong hệ thống.

1.2.Các công cụ giám sát dựa trên mã nguồn mở

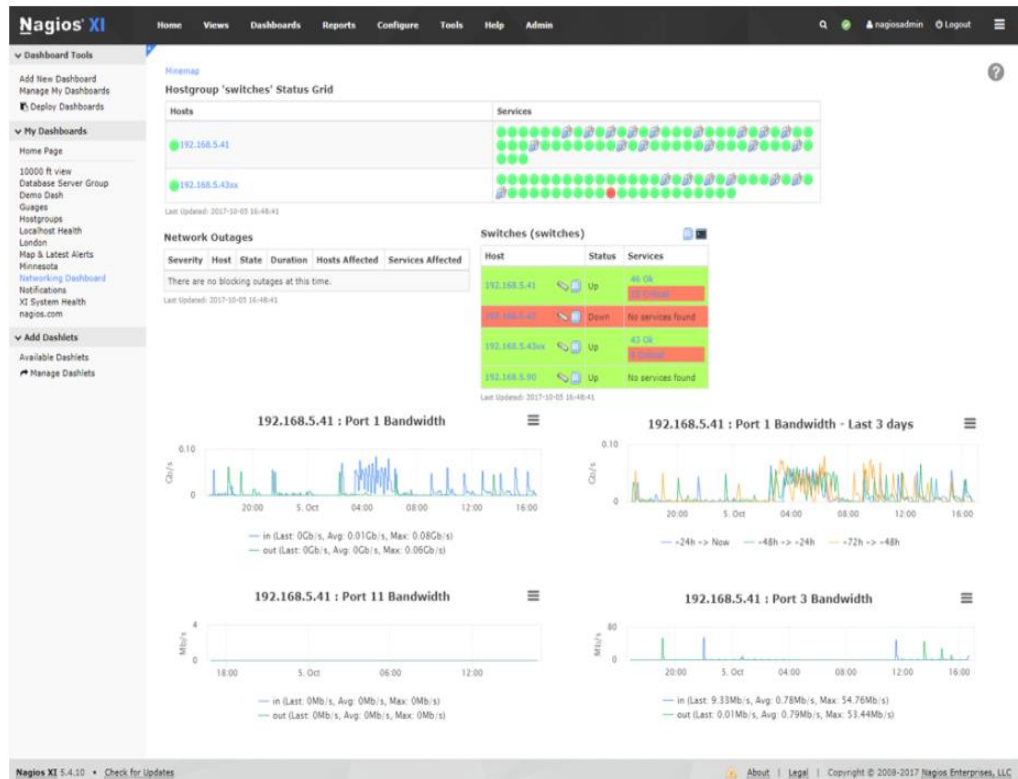
Cùng với việc phát triển của công nghệ thông tin, sự đầu tư cho hạ tầng mạng trong mỗi doanh nghiệp ngày càng tăng. Nên việc các mã nguồn mở xuất hiện ngày càng nhiều giúp các doanh nghiệp vừa và nhỏ có thể giám sát hệ thống mạng hiệu quả mà không tốn nhiều chi phí đơn giản trong việc triển khai như Nagios, Zabbix, Zenoss, Cacti,...

Trong đề tài này, chúng ta sẽ đề cập đến Nagios, một phần mềm mã nguồn mở với nhiều chức năng mạnh mẽ cho phép quản lý các thiết bị, dịch vụ trong hệ thống mạng. Mục tiêu của chúng ta trong bài báo này là giúp cho mọi người có cái nhìn tổng quan về một hệ thống giám sát mạng hoàn chỉnh, đồng thời đưa ra một giải pháp cụ thể đối với một hệ thống mạng dành cho doanh nghiệp.

2. TỔNG QUAN VỀ NAGIOS

2.1.Khái niệm về Nagios

- Nagios là một phần mềm mã nguồn mở hỗ trợ giám sát hoạt động của các thiết bị và các dịch vụ trong mạng. Nagios giúp giám sát hoạt động một số thiết bị trung tâm trong mạng như Server, Switch, Router,... Đồng thời kết hợp với bộ phận phát cảnh báo qua giao diện Web và âm thanh (Audio) phát cảnh báo trong trường hợp một thiết bị ngừng hoạt động hoặc một dịch vụ mạng ngừng hoạt động.



Hình 1: nagios

- Nagios giám sát các thiết bị mạng thông qua các giao thức SNMP, ... để theo dõi trạng thái hoạt động của các thiết bị. Đồng thời, Nagios còn cho phép thiết lập cơ chế giám sát hoạt động của các dịch vụ mạng. Các dịch vụ phổ biến được giám sát như: HTTP, FTP, SMTP, POP3, ...

2.2.Chức năng của Nagios

Nagios gồm 5 chức năng:

- Cảnh báo: Nagios gửi cảnh báo khi có thành phần cơ sở hạ tầng bất ổn định và phục hồi, cung cấp cho các quản trị viên thông báo của các sự kiện quan trọng. Cảnh báo có thể được gửi qua email, SMS, hay tùy chỉnh.



Hình 2: Hỗ trợ giám sát các thiết bị

- Ứng phó: Nhân viên CNTT có thể xác nhận cảnh báo và bắt đầu giải quyết sự cố ngưng hoạt động và kiểm tra hệ thống cảnh báo ngay lập tức. Cảnh báo có thể được gia tăng cho các nhóm khác nhau nếu thông báo không xác nhận một cách kịp thời.
- Báo cáo: Báo cáo cung cấp một hồ sơ lịch sử của sự cố ngưng hoạt động, sự kiện, thông báo, và phản ứng cảnh báo để xem xét. Sẵn có các báo cáo giúp đảm bảo SLAs của người dùng đang được đáp ứng.
- Bảo trì: Dự kiến thời gian ngừng làm việc ngăn cản các cảnh báo tổng quá trình bảo trì theo lịch trình và nâng cấp.



Hình 3: Bảo trì hệ thống

- Kế hoạch: Lập lịch đồ thị và báo cáo xu hướng và công suất cho phép người dùng cách định sự cần thiết nâng cấp cơ sở hạ tầng trước khi xảy ra sự cố.



Hình 4: Hỗ trợ lên kế hoạch

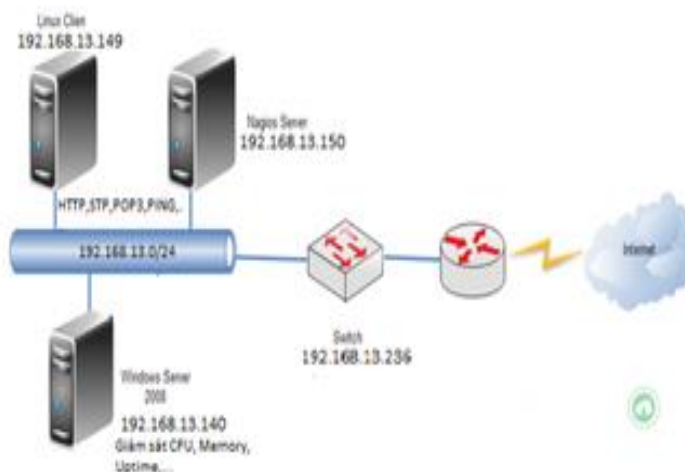
2.3.Đặc điểm của Nagios

- Giám sát toàn diện:
 - Khả năng để giám sát các ứng dụng, dịch vụ, hệ điều hành, giao thức mạng, hệ thống số liệu và các thành phần cơ sở hạ tầng với một công cụ duy nhất.
 - API mạnh mẽ cho phép giám sát dễ dàng các ứng dụng và tùy chỉnh các dịch vụ, và các hệ thống.
- Tầm nhìn:
 - Tập trung theo dõi toàn bộ cơ sở hạ tầng CNTT.
 - Chi tiết thông tin trạng thái hoạt động thông qua giao diện web.
- Nhận thức
 - Nhanh chóng phát hiện các sự cố ngưng hoạt động của cơ sở hạ tầng.
 - Cảnh báo có thể được gửi đến nhân viên kỹ thuật qua email hoặc tin nhắn SMS.
 - Khả năng leo thang đảm bảo các thông báo cảnh báo đến đúng người.
- Khắc phục vấn đề
 - Xác nhận cảnh báo cung cấp thông tin về các vấn đề được biết đến và ứng phó vấn đề.
 - Xử lý sự kiện cho phép tự động khởi động các ứng dụng thất bại và dịch vụ.

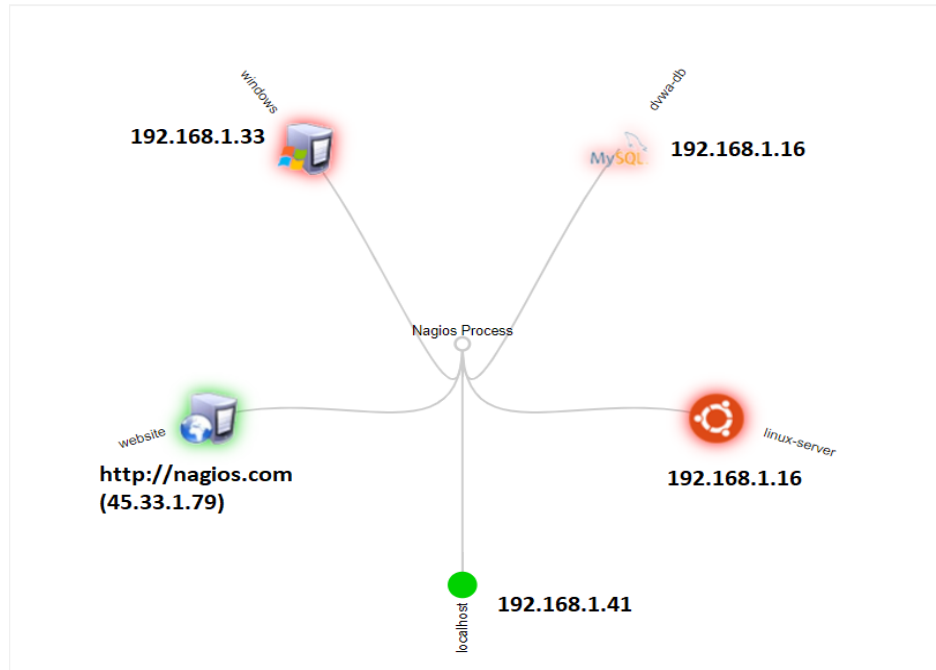
- Lập kế hoạch chủ động
 - Những phần hỗ trợ lập kế hoạch cho xu hướng và năng lực hoạt động đảm bảo người dùng nhận thức được sự xuống cấp của cơ sở hạ tầng.
 - Dự kiến thời gian ngưng hoạt động cho phép tắt cảnh báo trong quá trình nâng cấp cơ sở hạ tầng.
- Nhiều người dùng
 - Với chức năng này, cho phép nhiều người sử dụng có quyền truy cập xem tình trạng của cơ sở hạ tầng.
 - Những người xem riêng biệt chỉ thấy được cơ sở hạ tầng của họ.
- Kiến thức mở rộng
 - Hơn 10 năm phát triển hoạt động.
 - Ổn định, đáng tin cậy và nền tảng vững chắc.
 - Cân bằng để giám sát hàng ngàn điểm.
- Mã nguồn tùy chỉnh
 - Phần mềm nguồn mở.
 - Không giới hạn truy cập vào mã nguồn.
 - Phát hành theo giấy phép GPL (Giấy phép công cộng)..

2.4. Mô hình triển khai Nagios

Kiến trúc Nagios



Hình 5: Mô hình triển khai dự tính

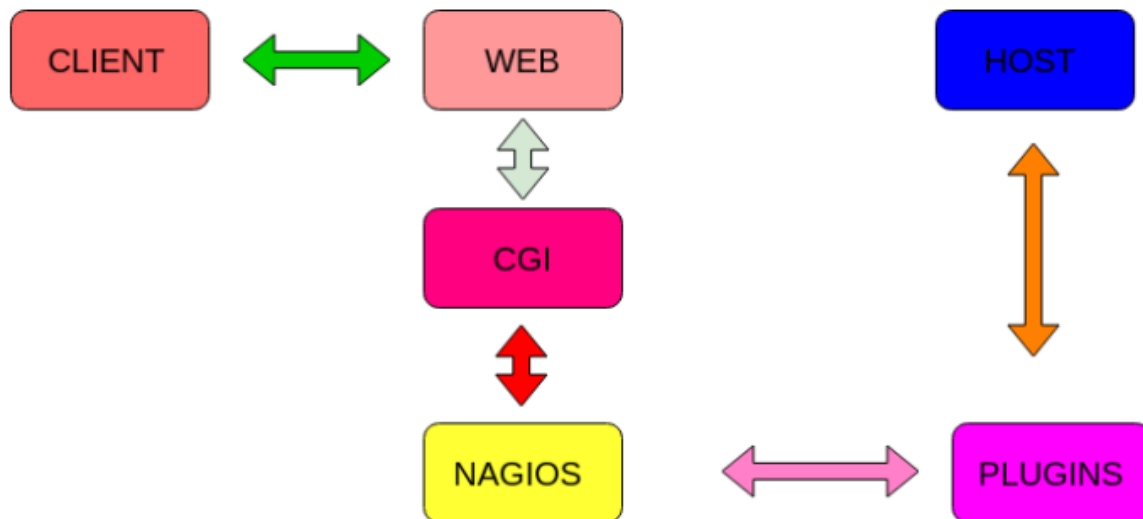


Hình 6: Mô hình triển khai thực tế

2.5.Kiến trúc và tổ chức hoạt động

- Cách thức hoạt động

Luồng hoạt động của nagios core



Hình 7: Luồng hoạt động của nagios

Bước 1: Client sẽ sử dụng giao thức http để tạo yêu cầu thông tin website cho Nagios Server

Bước 2: Web Server sẽ sử dụng CGI để lấy thông tin từ Nagios server

Bước 3: Nagios Server sẽ xem lại file cache. Nếu trong đó có thông tin mà client yêu cầu thì nó sẽ lập tức trả lại kết quả. Nếu không có nagios sẽ tạo ra một plugins để kiểm tra lại thông tin mà client yêu cầu

Bước 4: Plugins sẽ check thông tin theo yêu cầu và sau đó trả lại thông tin lại cho Nagios Server

Bước 5: Sau khi được nhận thông tin từ plugins thì Nagios Server sẽ lưu trữ thông tin đó vào một File hoặc một DB do cài đặt của người quản trị. Và đồng thời nó sẽ lưu trữ thông tin này vào File Cache nếu người quản trị có sử dụng chức năng của file này

Bước 6: Nagios sẽ xác định những việc phải làm dựa trên thông tin được trả về từ Nagios. Có cần cảnh báo hay không và đánh giá trạng thái của các host hay service. Rồi sau đó trả lại thông tin cho webserver

Bước 7: Web Server sẽ sử dụng lại giao thức http trả lại thông tin mà client yêu cầu.

2.6. Khả năng giám sát thiết bị

2.6.1. Khả năng giám sát của Nagios:

- Kết nối đến thiết bị(ping thiết bị).
- Trạng thái up/down của các cổng.
- Sử dụng băng thông,lưu lượng trên các cổng.
- Tỷ lệ mất gói tin, trung bình trễ trọn vòng(RTA).

2.6.2. **Giám sát thông tin trạng thái qua SNMP:** Nếu Switch hay Router của người dùng hỗ trợ SNMP, họ có thể giám sát rất nhiều thông tin bằng check_snmp plugin. Bổ xung định nghĩa dịch vụ bên dưới để định nghĩa uptime(thời gian chạy liên tục) của switch.

2.6.3. **Giám sát dịch vụ mạng:** Đối với các dịch vụ mạng như HTTP, POP3, IMAP, FTP, SSH... là các dịch vụ dùng chung, công khai. Nagios thường giám sát được trạng thái của các dịch vụ này mà không cần bất cứ yêu cầu truy cập đặc biệt nào.

Không như các dịch vụ riêng, Nagios không thể giám sát được nếu như không có các agent trung gian. Ví dụ các dịch vụ có liên quan đến host như là tải CPU, tình trạng sử dụng bộ nhớ trong, ổ đĩa, ... Vì những thông tin này thường không được công khai với bên ngoài và yêu cầu quyền truy cập.

2.6.4. Giám sát Web Server: Nagios sử dụng plugin `check_http` trong việc giám sát dịch vụ HTTP trên web server. `check_http` có thể nhận biết được các thông tin sau:

- Thời gian trả lời của Web Server.
- Mã lỗi trả về của dịch vụ HTTP (403 : không tìm thấy tệp, 404: lỗi xác thực).
- Nội dung chuỗi trả về của HTTP có chứa chuỗi s cho trước không.
- Một URL nào đó có còn nằm trên Web Server hay không.

2.6.5. Giám sát Proxy Server, File Server, Mail Server, dịch vụ POP3, IMAP,...:

2.7. Các Agent của Nagios

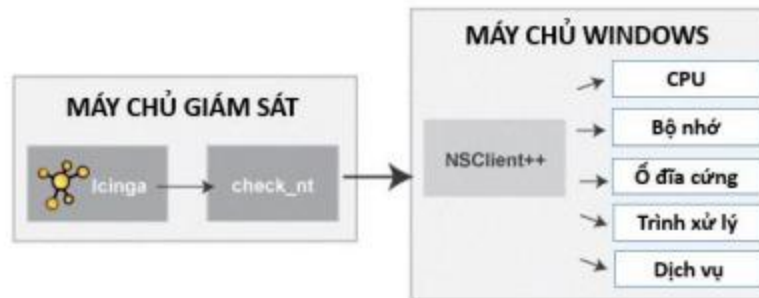
2.7.1. NRPE: Nagios Remote Plugin Executor (NRPE) cung cấp cho Nagios với khả năng được giám sát từ xa bởi các máy chủ. NRPE gồm 2 phần, một là plugin nằm trên máy chủ, hai là các tiến trình chạy trên các máy được giám sát. Nagios sử dụng `check_nrpe` để yêu cầu tiến trình NRPE chạy kiểm tra trên các máy ở xa. Nếu các máy ở xa được cấu hình để cho phép điều này thì nó sẽ chạy phần hỗ trợ và trả kết quả lại cho `check_nrpe` trên máy chủ Nagios. NRPE dùng cho Linux Server.



Hình 8: Nagios giám sát host hệ điều hành linux

2.7.2. NSClient++: Nhằm mục đích trở thành một trình nền giám sát đơn giản nhưng mạnh mẽ và linh hoạt. NSClient++ được xây dựng cho Nagios / Icinga / Naemon, và nó có thể được sử dụng trong nhiều trường hợp khác mà người sử dụng muốn nhận / phân phối số liệu kiểm

tra. Hoàn toàn có thể sử dụng nó độc lập cũng như hệ thống giám sát cốt lõi mặc dù điều đó không được khuyến khích vì nó vẫn còn khá hạn chế. NSClient++ dùng cho Windows

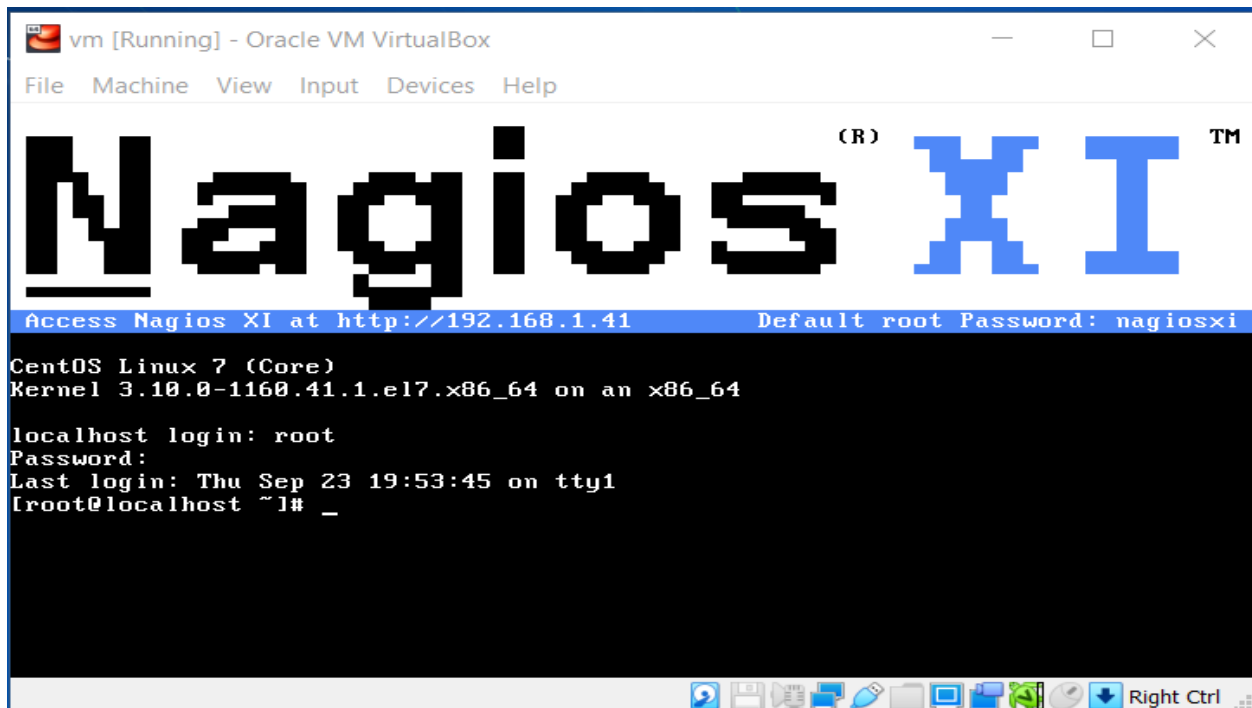


Hình 9: Nagios giám sát host hệ điều hành windows

2.7.3. Ngoài ra còn có NRDP, NCPA.

III. CÀI ĐẶT NAGIOS

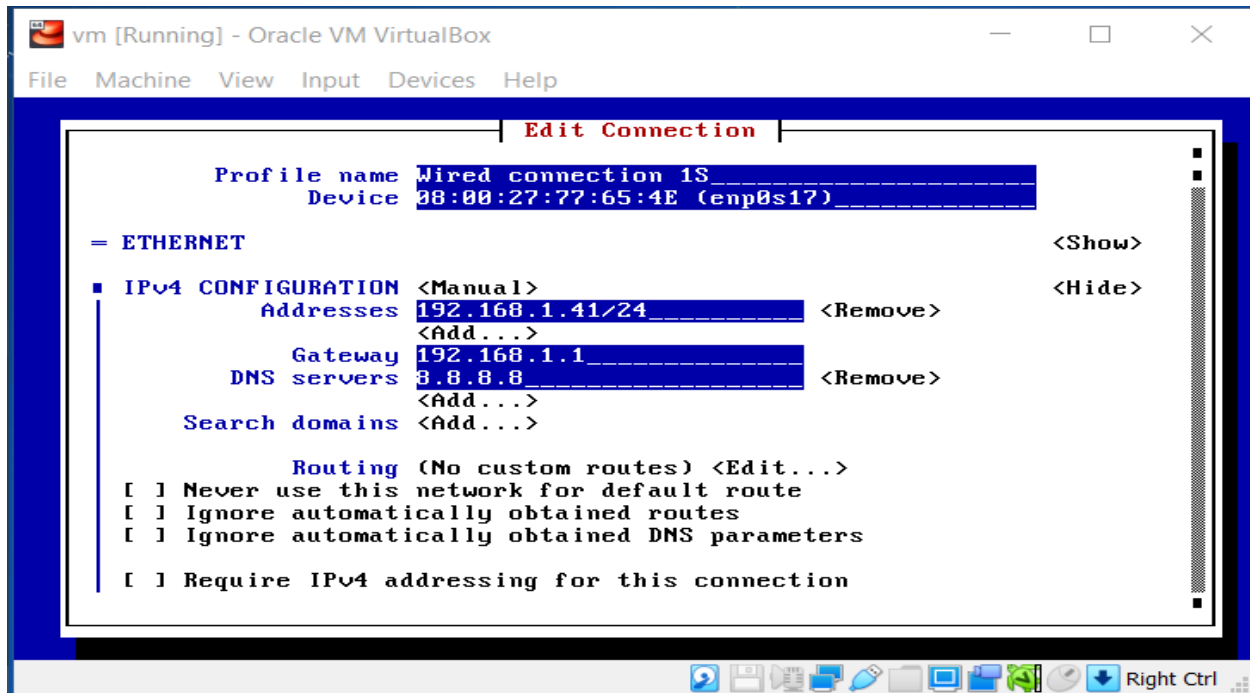
1. Cài đặt nagios vào Virtualbox



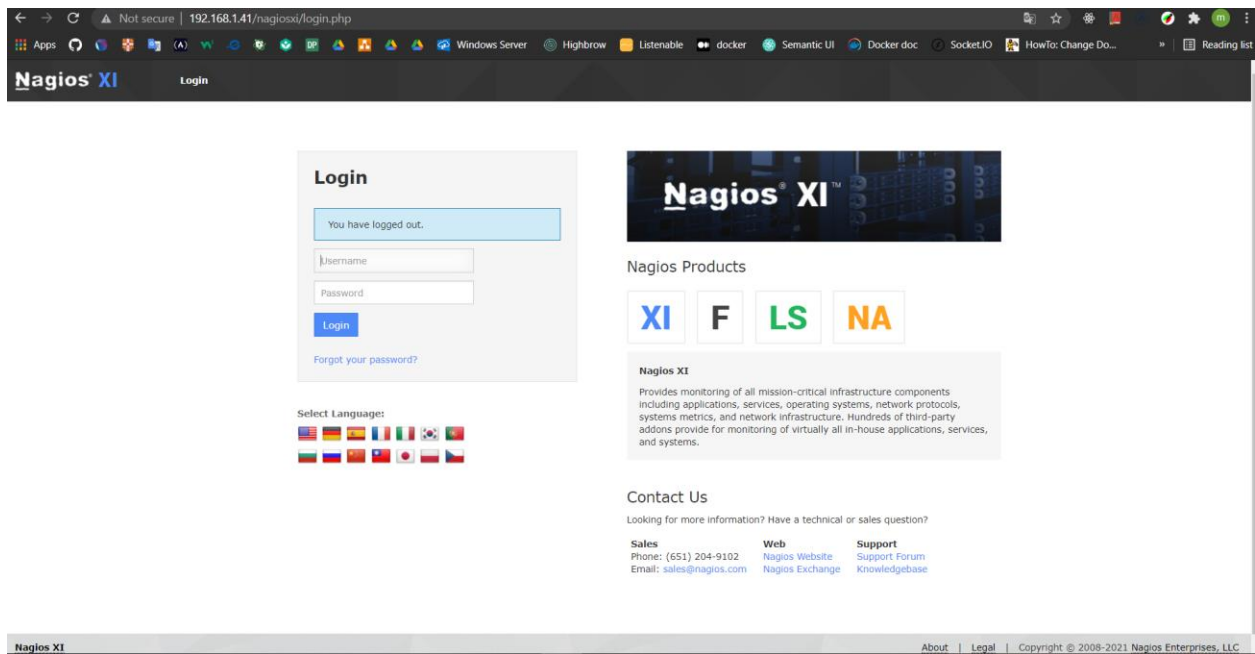
Hình 10: Màn hình đăng nhập nagios

Sau khi cài đặt xong đăng nhập vào với tài khoản root/nagiosxi

Dùng lệnh nmtui để đặt lại địa chỉ IP cho nagios



Hình 11: Đặt IP tĩnh cho máy chủ giám sát nagios

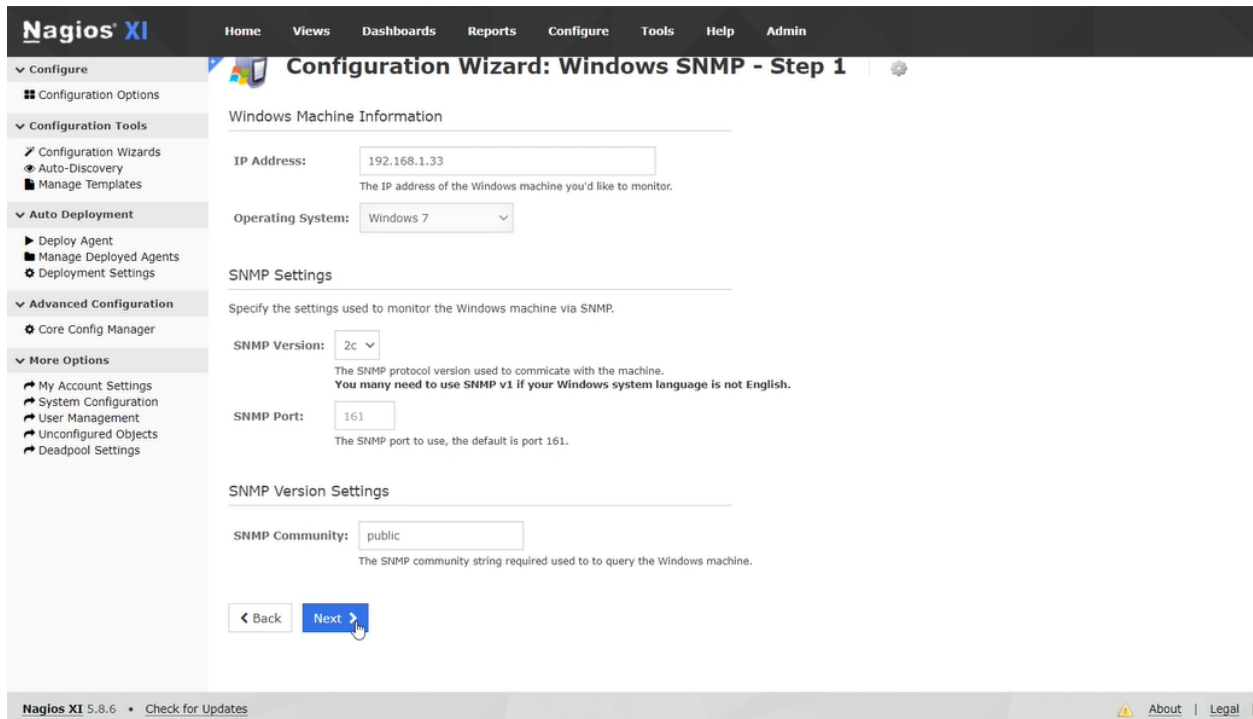


Hình 12: Màn hình đăng nhập quản lý nagios website

2. Thêm các host vào nagios để thực hiện giám sát

2.1.Windows host:

Sau khi enable dịch vụ snmp trên máy windows thì vào nagios -> configuration wizards -> windows snmp, ...



The screenshot shows the Nagios XI Configuration Wizard for Windows SNMP. The interface includes a top navigation bar with links like Home, Views, Dashboards, Reports, Configure, Tools, Help, and Admin. A left sidebar contains a tree view with categories like Configure, Configuration Tools, Auto Deployment, Advanced Configuration, and More Options. The main content area is titled 'Configuration Wizard: Windows SNMP - Step 1' and contains the following sections:

- Windows Machine Information:**
 - IP Address:** 192.168.1.33 (with a note: 'The IP address of the Windows machine you'd like to monitor.')
 - Operating System:** Windows 7 (dropdown menu)
- SNMP Settings:**
 - SNMP Version:** 2c (dropdown menu, with a note: '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 (with a note: 'The SNMP port to use, the default is port 161.')
- SNMP Version Settings:**
 - SNMP Community:** public (with a note: 'The SNMP community string required used to to query the Windows machine.')

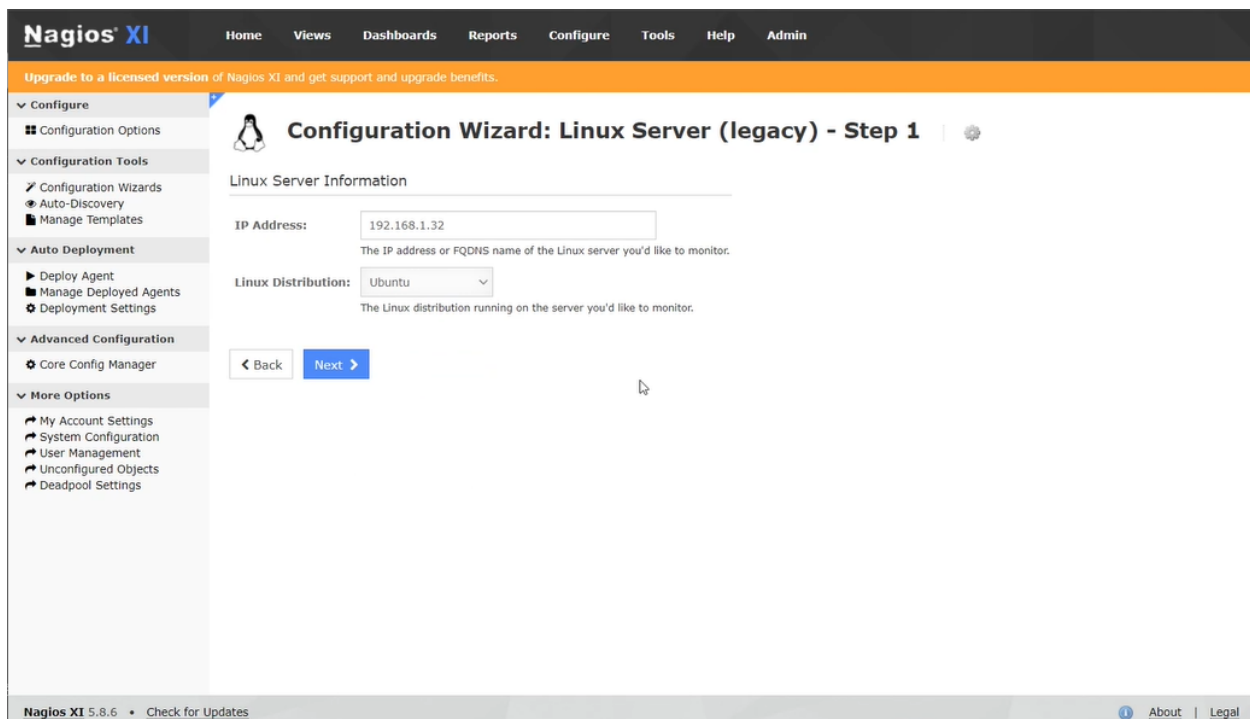
At the bottom of the form are two buttons: 'Back' and 'Next'.

Hình 13: Thực hiện cấu hình giám sát host windows

2.2.Linux host:

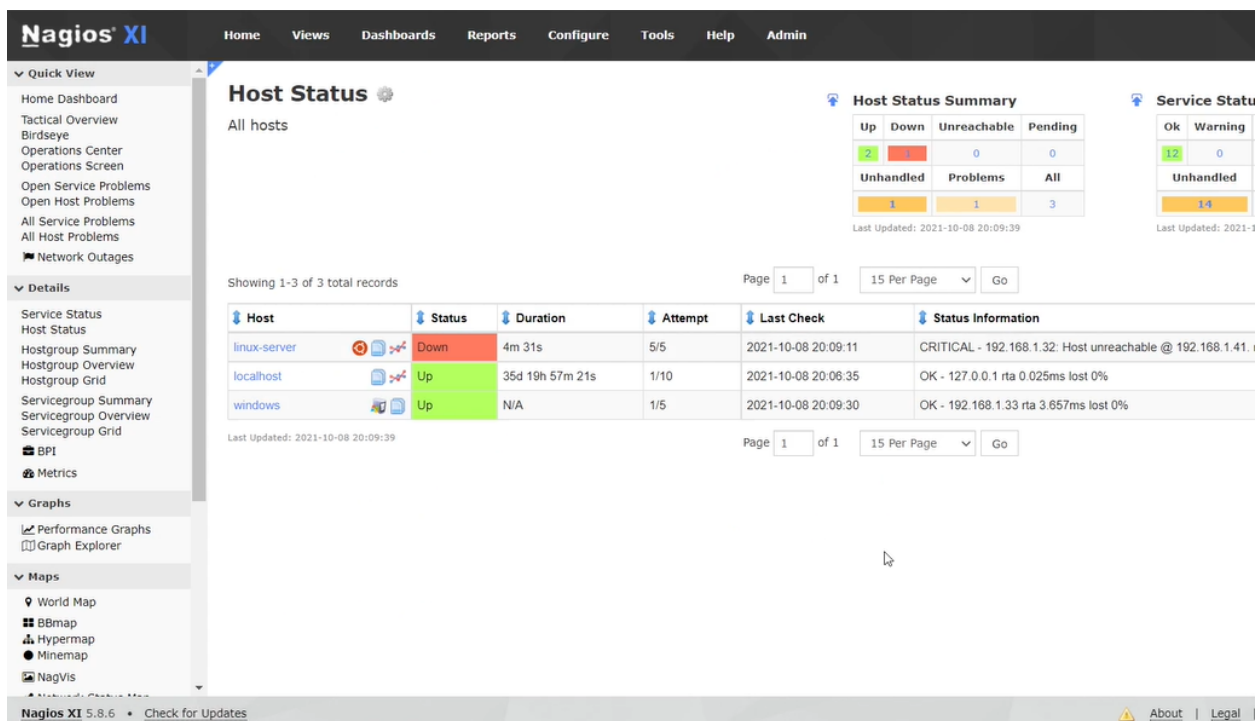
- Trên máy linux server đã deploy NRPE

nagios -> configuration wizards -> linux snmp, ...



Hình 14: Thực hiện cấu hình giám sát host linux server

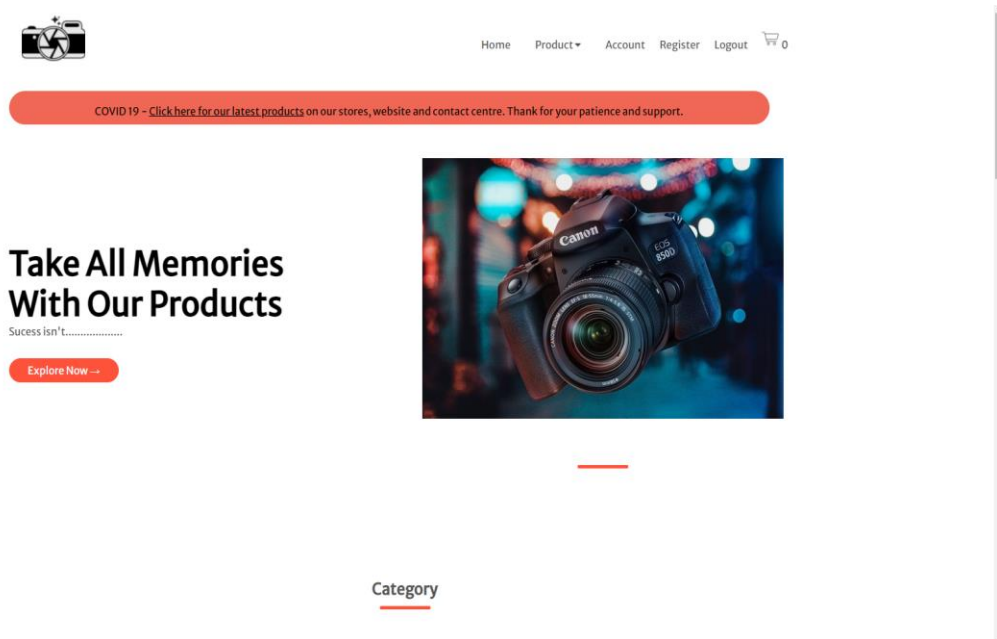
- Kết quả sau khi thực hiện:



Hình 15: Kết quả sau khi thực hiện

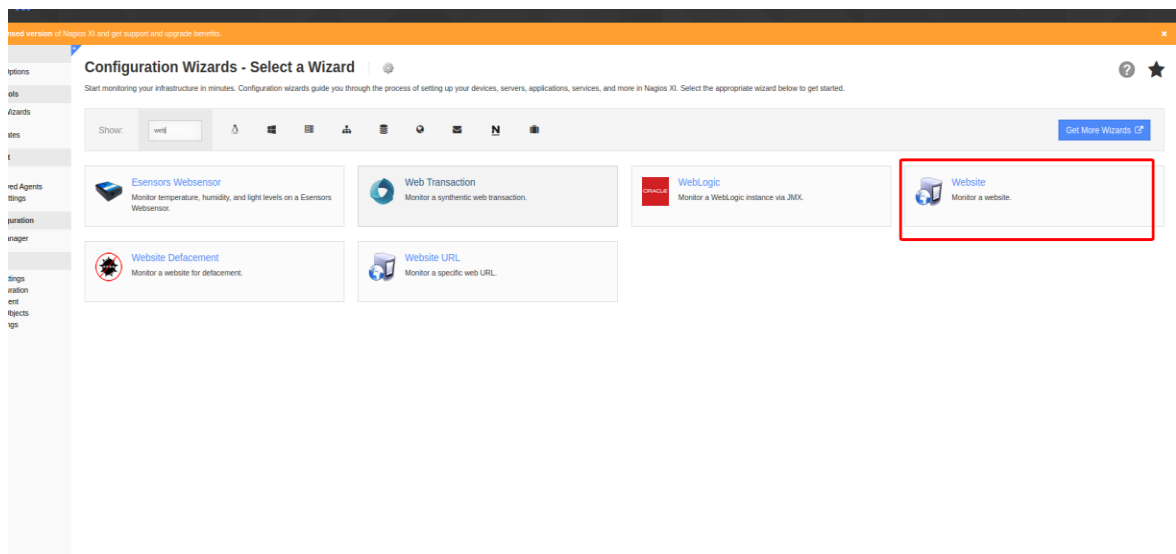
2.3. Cấu hình giám sát dịch vụ Web

1. Chuẩn bị một trang web sẽ theo dõi : <http://gentle-bayou-09243.herokuapp.com/>



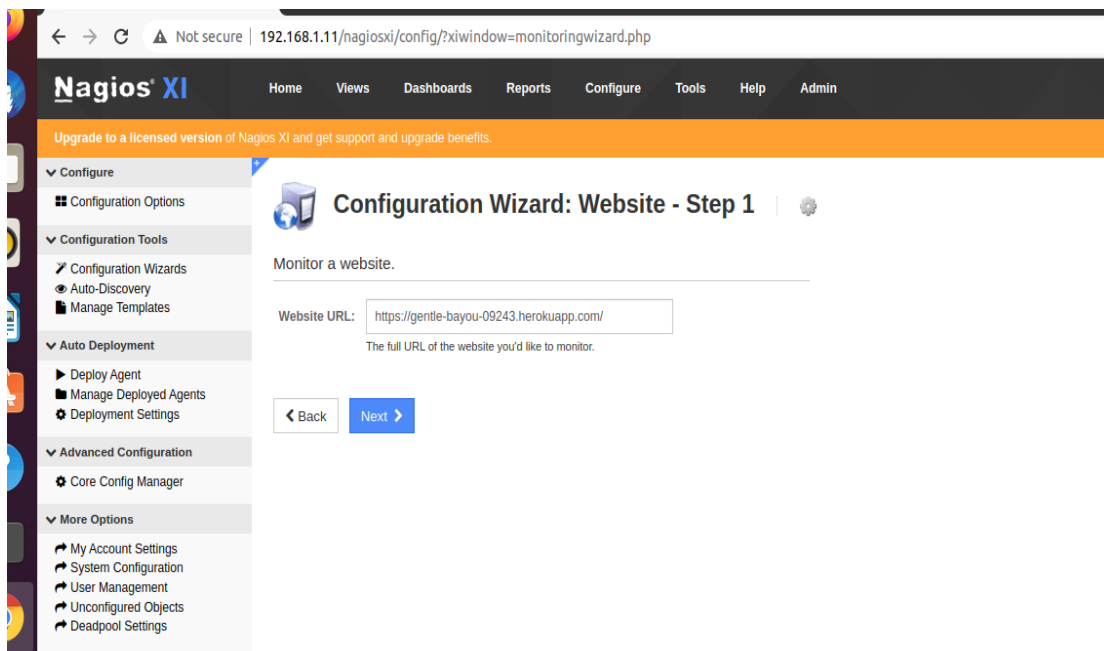
Hình 16: Website đã chuẩn bị để giám sát

Vào Nagios XI và giám sát theo Website



Hình 17: Thực hiện cấu hình giám sát website

Nhập đường dẫn URL và chọn vào next :



Hình 18: Thực hiện cấu hình giám sát website

Chọn các dịch vụ muốn theo dõi : Ví dụ : HTTP, Ping, DSN resolution

Website Details

Website URL:

Host Name:
The name you'd like to have associated with this website.

IP Address:
The IP address associated with the website fully qualified domain name (FQDN).

Website Options

Use SSL: ☒ Monitor the website using SSL/HTTPS.

Port:
The port to use when contacting the website.

On Redirect:
How to handle redirected pages. sticky is like follow but will stick to the specified IP address. stickyport ensures the port stays the same.

Credentials:
Basic authentication only. The username and password to use to authenticate to the website (optional)

Website Services

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

☒ **HTTP**
Includes basic monitoring of the website to ensure the web server responds with a valid HTTP response.

☒ **Ping**
Monitors the website server with an ICMP ping. Useful for watching network latency and general uptime of your web server. Not all web servers support this.

☒ **DNS Resolution**
Monitors the website DNS name to ensure it resolves to a valid IP address.

Hình 19: Chọn các dịch vụ cần giám sát

Website Services

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

☒ **HTTP**
Includes basic monitoring of the website to ensure the web server responds with a valid HTTP response.

☒ **Ping**
Monitors the website server with an ICMP ping. Useful for watching network latency and general uptime of your web server. Not all web servers support this.

☒ **DNS Resolution**
Monitors the website DNS name to ensure it resolves to a valid IP address.

☒ **DNS IP Match**
Monitors the website DNS name to ensure it resolves to the current known IP address. Helps ensure your DNS doesn't change unexpectedly, which may mean a security breach has occurred.

☐ **Web Page Content**
Monitors the website to ensure the specified string is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly.
Content String To Expect:

☐ **Web Page Regular Expression Match**
Monitors the website to ensure the specified regular expression is found in the content of the web page. A content mismatch may indicate that your website has experienced a security breach or is not functioning correctly.
Regular Expression To Expect:

☒ **SSL Certificate**
Monitors the expiration date of the website's SSL certificate and alerts you if it expires within the specified number of days. Helps ensure that SSL certificates don't inadvertently go un-renewed.
Days To Expiration:

Hình 20: Chọn các dịch vụ giám sát

Sau khi chọn các dịch vụ muốn giám sát , sau đó bấm Next để tiếp tục :

Configuration Wizard: Website - 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 minutes.

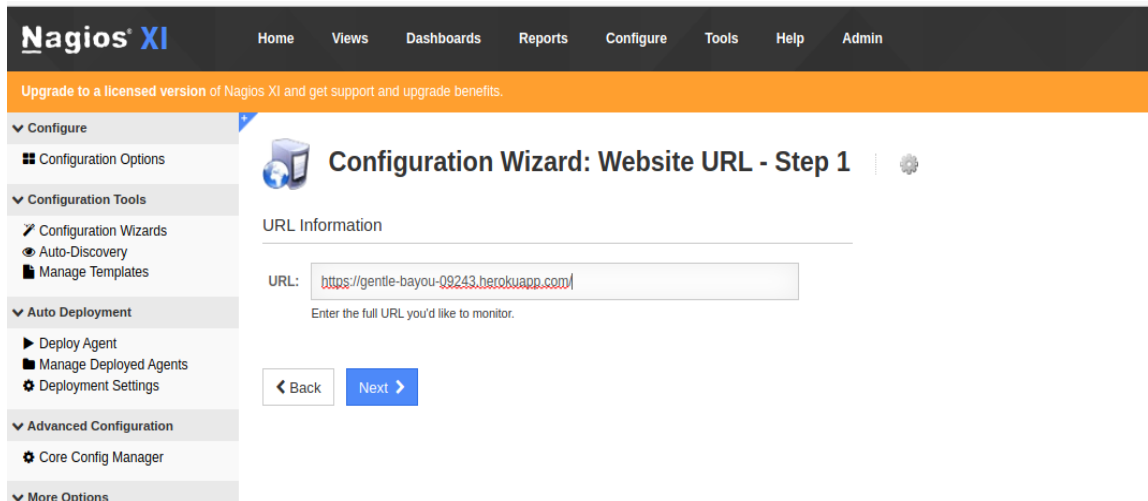
When a potential problem is first detected:

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

Hình 21: Chọn finish để hoàn tất quá trình cấu hình

Tại bước ba chọn Finish để hoàn thành

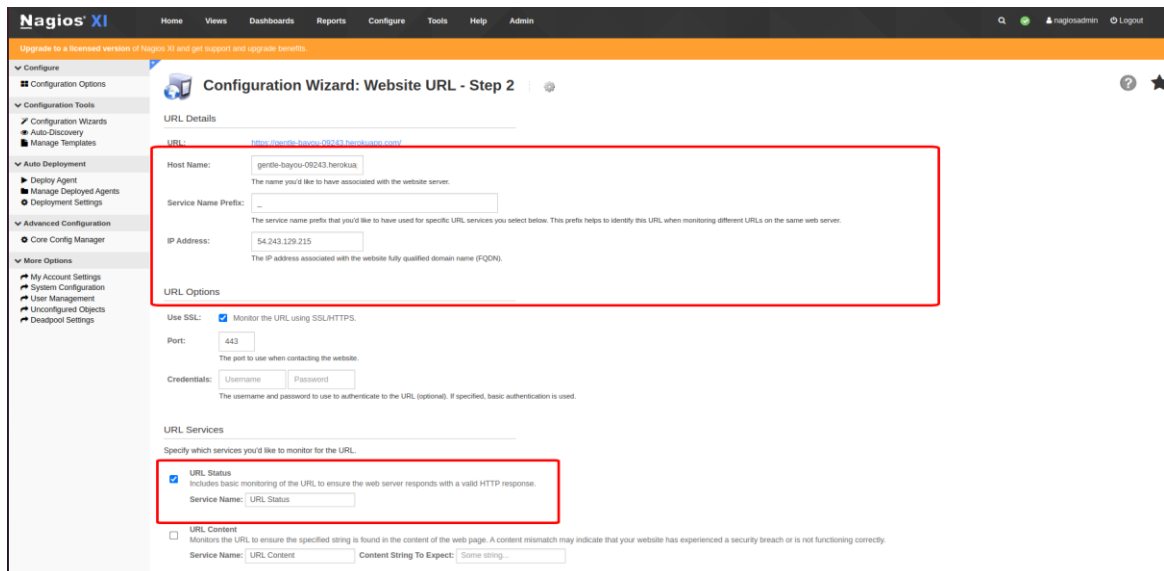
-Tiếp tục chọn vào cấu hình Website URL để cấu hình



The screenshot shows the Nagios XI interface. The top navigation bar includes links for Home, Views, Dashboards, Reports, Configure, Tools, Help, and Admin. Below the navigation bar is a banner for upgrading to a licensed version. The left sidebar contains a menu with categories like Configure, Configuration Tools, Auto Deployment, Advanced Configuration, and More Options. The main content area is titled 'Configuration Wizard: Website URL - Step 1' and shows the 'URL Information' section. A text input field for 'URL:' contains the value 'https://gentle-bayou-09243.herokuapp.com/'. Below the input field is a prompt 'Enter the full URL you'd like to monitor.' and two buttons: 'Back' and 'Next'.

Hình 22: Cấu hình Website URL

Nhập đường dẫn và chọn Next để tiếp tục :





The screenshot shows the Nagios XI interface for 'Configuration Wizard: Website URL - Step 2'. The left sidebar is the same as in Step 1. The main content area is titled 'URL Details' and contains several sections. The 'URL' section has a text input field for 'URL:' with the value 'https://gentle-bayou-09243.herokuapp.com/'. Below this is the 'Host Name' section with a text input field for 'Host Name:' containing 'gentle-bayou-09243.herokuapp.com'. The 'Service Name Prefix' section has a text input field for 'Service Name Prefix:' containing '-'. The 'IP Address' section has a text input field for 'IP Address:' containing '54.243.129.215'. The 'URL Options' section has a checkbox for 'Use SSL:' which is checked, and a text input field for 'Port:' containing '443'. The 'URL Services' section has a checkbox for 'URL Status' which is checked, and a text input field for 'Service Name:' containing 'URL Status'. The 'URL Content' section has a checkbox for 'URL Content' which is unchecked, and a text input field for 'Service Name:' containing 'URL Content' and a text input field for 'Content String To Expect:' containing 'Some string...'. A red box highlights the 'URL Status' section.

Hình 23: Cấu hình Website URL

Chọn địa chỉ IP và tick vào URL status để giám sát trạng thái URL

Sau đó nhấn chọn Next để tiếp tục :

 **Configuration Wizard: Website URL - 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 minutes.

When a potential problem is first detected:

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

Hình 24: Chọn finish để hoàn tất

Tại bước 3 chọn Finish để hoàn thành

- Kết quả :

Host Status Detail

gentle-bayou-09243.herokuapp.com

Services

Service Status for this Host

Service

Status

Duration

Attempt

Last Check

Status Information

URL Content

Ok

1m 51s

1/5

2021-10-26 07:42:02

HTTP OK: HTTP/1.1 200 OK - 12828 bytes in 2.567 second response time

URL Content Regex

Critical

54s

1/5

2021-10-26 07:41:53

CRITICAL - Socket timeout

URL Status

Ok

11s

1/5

2021-10-26 07:42:36

HTTP OK: HTTP/1.1 200 OK - 12828 bytes in 2.862 second response time

DNS IP Match

Critical

24m 57s

5/5

2021-10-26 07:37:48

DNS CRITICAL - expected '54.224.34.30' but got '34.201.81.34,54.208.186.182,54.224.34.30,54.243.129.215'

DNS Resolution

Ok

28m 40s

1/5

2021-10-26 07:39:05

DNS OK: 0.044 seconds response time, gentle-bayou-09243.herokuapp.com returns 34.201.81.34,54.208.186.182,54.224.34.30,54.243.129.215

HTTP

Ok

12m 33s

1/5

2021-10-26 07:41:08

HTTP OK: HTTP/1.1 200 OK - 12828 bytes in 7.474 second response time

Ping

Critical

24m 4s

5/5

2021-10-26 07:38:50

CRITICAL - gentle-bayou-09243.herokuapp.com: rta nan, lost 100%

SSL Certificate

Ok

18m 2s

1/5

2021-10-26 07:40:49

SSL OK - Certificate '*herokuapp.com' will expire in 247 days on 2022-06-30 16:59 -0700PDT.

Web Page Content

Ok

1m 3s

1/5

2021-10-26 07:41:44

HTTP OK: HTTP/1.1 200 OK - 12828 bytes in 7.243 second response time

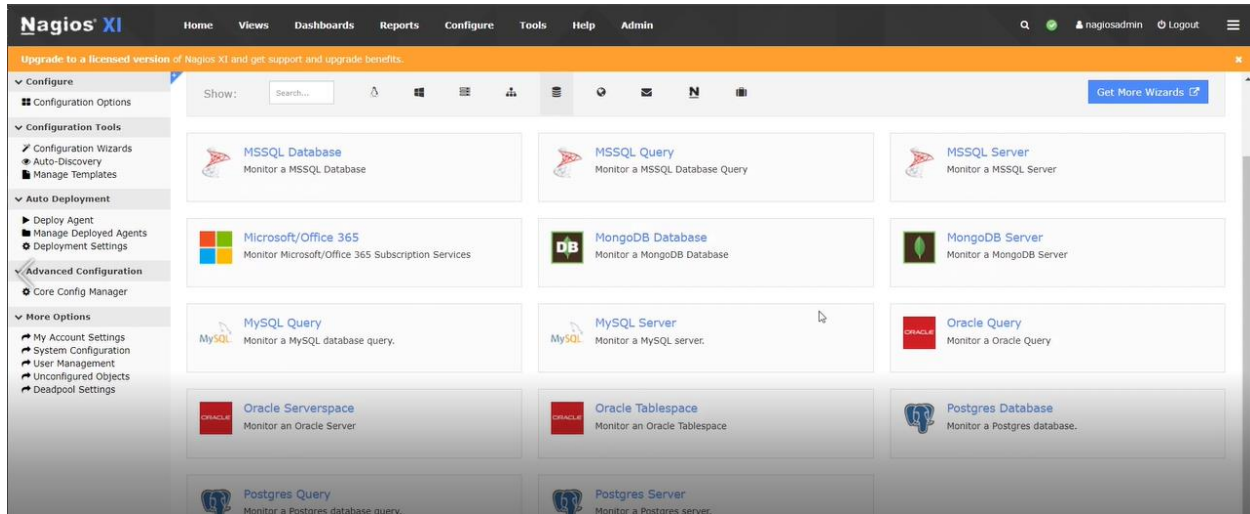
Last updated: 2021-10-26 07:42:47

Hình 25: Kết quả

19

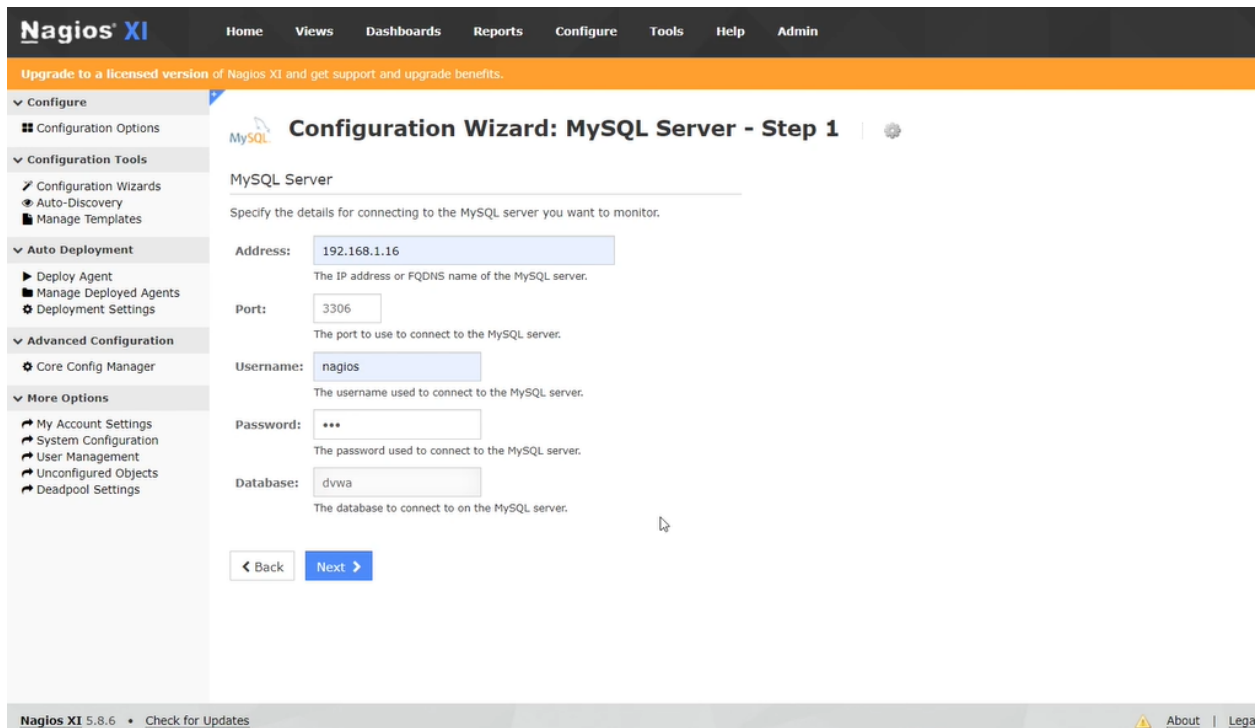
2.4. Giám sát dịch vụ cơ sở dữ liệu Mysql

- Chọn mục configure mysql server:



Hình 26: Chọn MySQL Server

- Nhập thông tin IP, username, password và database muốn thực hiện giám sát thông qua nagios:



Hình 27: Nhập IP, Username, Password, Database

- Cấu hình các thông số giám sát theo nhu cầu:

The screenshot shows the Nagios XI interface for configuring MySQL server metrics. The left sidebar contains navigation links under 'Configure', 'Configuration Tools', 'Auto Deployment', 'Advanced Configuration', and 'More Options'. The main content area is titled 'MySQL Server Metrics' and includes a sub-header 'Specify the metrics you'd like to monitor on the MySQL server.' Below this, several metrics are listed with checkboxes and input fields for thresholds:

- Connection Time:** Monitor the time it takes to connect to the server. Thresholds: 1 sec (warning), 5 sec (critical).
- Uptime:** Monitor the time the MySQL server has been running. Lower numbers are worse and are indicative of the server having been restarted. Thresholds: Low: 10 min, High: [] min (warning); Low: 5 min, High: [] min (critical).
- Open Connections:** Monitor the number of currently open connections. Thresholds: 10 (warning), 20 (critical).
- Thread Cache Hitrate:** Monitor the thread cache hit rate. Thresholds: Low: 90 %, High: [] % (warning); Low: 80 %, High: [] % (critical).
- Query Cache Hitrate:** Monitor the query cache hit rate. Thresholds: Low: 90 %, High: [] % (warning); Low: 80 %, High: [] % (critical).
- MyISAM Key Cache Hitrate:** Monitor the MyISAM key cache hit rate.

The footer shows 'Nagios XI 5.8.6' and a 'Check for Updates' link.

Hình 28: Chọn các thông số giám sát

- Chọn finish để hoàn tất quá trình cấu hình:

The screenshot shows the Nagios XI interface for the 'Configuration Wizard: MySQL Server - Step 3'. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Monitoring Settings' and includes a sub-header 'Define basic parameters that determine how the host and service(s) should be monitored.' Below this, there are two sections for monitoring settings:

- 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.

At the bottom, there are three buttons: '< Back', 'Next >', and a green 'Finish' button with a checkmark icon.

The footer shows 'Nagios XI 5.8.6' and a 'Check for Updates' link.

Hình 29: Chọn finish để hoàn tất

- ❖ Ý nghĩa các thông số giám sát dịch vụ Mysql:
- Connection time: giám sát thời gian cần để kết nối đến server
 - Uptime: giám sát thời gian mysql server đang chạy.
 - Open connections: giám sát số connection đang mở
 - Thread cache Hitrate: giám sát tỉ lệ cache của các tiến trình đang chạy
 - Query Cache Hitrate: giám sát tỉ lệ cache của các truy vấn