



Install and configure Nagios on Ubuntu 22.04

Services et Administration des Réseaux

Requirements

- A virtual machine running Ubuntu 22.04.
- Root or Sudo Access: To execute administrative tasks, you'll need either root access or a user account with sudo privileges.

Goals

- Configure Nagios under Ubuntu 22.04

Introduction

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Three significant versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security.

An SNMP-managed network consists of three key components:

- Managed devices
- Agent – software which runs on managed devices
- Network management station (NMS) – software which runs on the manager.

Step1: Update and Upgrade

The first step is to ensure that your system is up to date. Open a terminal and run the following commands:

```
# sudo apt update && apt upgrade -y
```

Step2: Install Prerequisites

Nagios has specific software prerequisites that need to be installed on your Ubuntu 22.04 machine before you can install and configure Nagios itself. By installing all these prerequisites, you ensure that your Ubuntu 22.04 system has all the necessary dependencies to run Nagios optimally and enable efficient monitoring of your systems and services.

```
# sudo apt install build-essential apache2 php libgd-dev libapache2-mod-php libperl-dev libssl-dev daemon wget
```

Step 3: Create a Nagios User and Group

Nagios should run as a separate user and group. Create them with the following commands:

```
# sudo useradd nagios  
  
# sudo groupadd nagcmd  
  
# sudo usermod -a -G nagcmd nagios  
  
# sudo usermod -a -G nagios,nagcmd www-data
```

Step 4: Download Nagios on Ubuntu

We are performing a manual installation. To do so, download the tar.gz file via the following command.

```
# cd ~  
  
# wget https://github.com/NagiosEnterprises/nagioscore/releases/download/nagios-4.5.9/nagios-4.5.9.tar.gz
```

Step 5: Extract downloaded tar.gz file

Once you have downloaded the Nagios source code, you can extract its contents and proceed with the compilation and installation.

The file is available as “nagios-4.4.6.tar.gz”. We executed the following command to extract it.

```
# tar -xzf nagios-4.5.9.tar.gz
```

Step6: Compile Nagios Core

Make sure, you are inside the directory where the Nagios is extracted. Next, configure Nagios on Ubuntu and compile it:

```
# cd nagios-4.5.9  
  
# sudo ./configure --with-nagios-group=nagios --with-command-group=nagcmd  
  
# sudo make all
```

Step7: Install Nagios Core Binaries and Web Interface Files

```
# sudo make install  
  
# sudo make install-commandmode  
  
# sudo make install-init  
  
# sudo make install-config  
  
# sudo /usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-available/nagios.conf  
  
# sudo cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/  
  
# sudo chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers
```

Step8: Download, Extract and Install Nagios on Ubuntu Plugins

```
# wget https://nagios-plugins.org/download/nagios-plugins-2.1.2.tar.gz  
  
# tar -xzf nagios-plugins*.tar.gz  
  
# cd nagios-plugins-2.1.2/  
  
# ./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl  
  
# sudo make  
  
# sudo make install
```

Step9: Configuring Nagios

1- uncomment line 51 for the host monitor configuration. cfg_dir=/usr/local/nagios/etc/servers

Save and exit.

```
# sudo gedit /usr/local/nagios/etc/nagios.cfg
```

2- Add a new folder named servers:

```
# sudo mkdir -p /usr/local/nagios/etc/servers
```

3- The Nagios contact can be configured in the contact.cfg file. To open it use:

```
# sudo gedit /usr/local/nagios/etc/objects/contacts.cfg
```

Then replace the default email with your own email.

Step 10: Configuring apache2

1- Enable the Nagios virtualhost

```
# sudo ln -s /etc/apache2/sites-available/nagios.conf /etc/apache2/sites-enabled/
```

2- Nagios utilizes the Apache web server as part of its setup for hosting its web interface. To make sure everything works properly, you need to enable specific Apache modules and then restart the Apache service.

```
# sudo a2enmod rewrite cgi
```

```
# sudo systemctl restart apache2
```

- The a2enmod command enables the required Apache modules for Nagios.

Step 11: Set Nagios Admin Password

You will be prompted to set a password for the user 'nagiosadmin.' Please make note of this password as it will be used to access the Nagios web interface.

```
# sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Step 12: Start Nagios and Apache Services

By executing these commands, you'll have both Nagios and Apache running on your Ubuntu system, allowing you to access the Nagios web interface and start monitoring your infrastructure.

```
# sudo systemctl enable nagios  
  
# sudo systemctl enable apache2  
  
# sudo systemctl restart nagios  
  
# sudo systemctl restart apache2
```

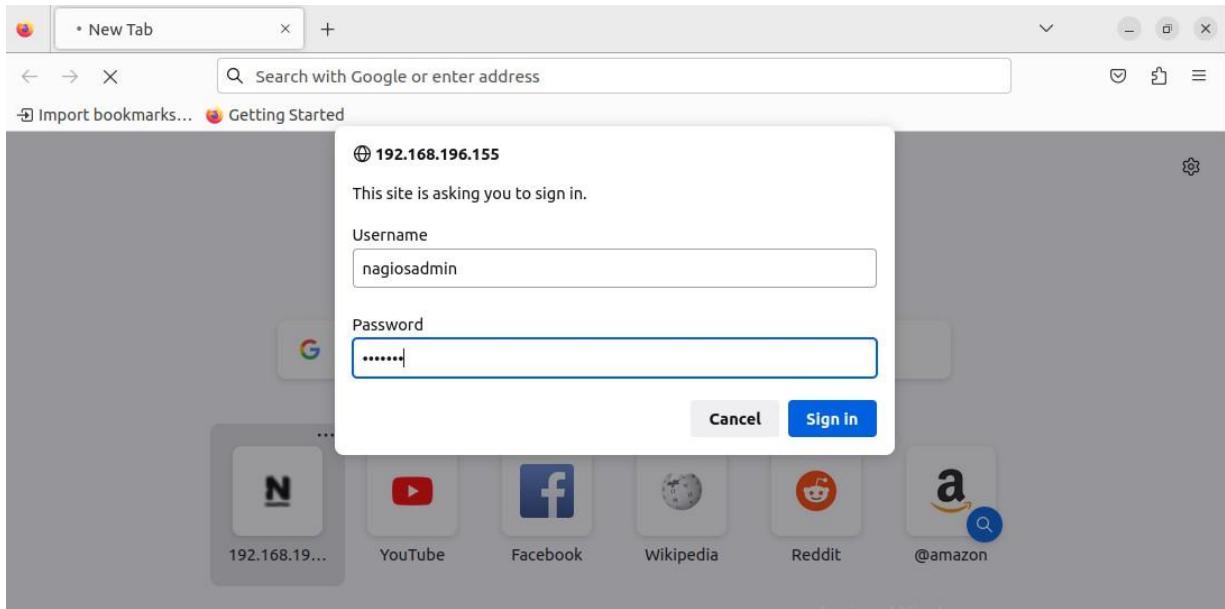
Step 13: Access Nagios Web Dashboard

In the address bar of the web browser, enter the IP address or hostname of your Ubuntu server, followed by “/nagios”.

```
http://your_server_ip_or_hostname/nagios
```

Replace “your_server_ip” with the actual IP address or hostname of your Ubuntu server where Nagios is installed

Log in to the web interface with the username nagiosadmin and the password you set during installation. (By default, the username is “nagiosadmin.”)



In the above screenshot, you will only see the localhost. To monitor remote machines, you will need to add the host to Nagios.

Step 14: Adding the host to Nagios

Open a terminal and navigate to the directory where Nagios configurations are stored. The default path is /usr/local/nagios/etc/servers

You should already have a host.cfg file or create one if it doesn't exist.

In the host.cfg file, you need to define the host you want to monitor. Here's an example configuration:

```

host.cfg
/usr/local/nagios/etc/servers

1 define host {
2     use          linux-server
3     host_name   machine-physique
4     alias        machine physique
5     address     192.168.1.30
6     max_check_attempts 3
7     check_period    24x7
8     notification_interval 30
9     notification_period 24x7
10
11 }
12
13 define host {
14     use          linux-server
15     host_name   web-server-vm
16     alias        serveur web déployé sur une 2ème vm
17     address     192.168.196.153
18     max_check_attempts 3
19     check_period    24x7
20     notification_interval 30
21     notification_period 24x7
22
23 }

```

```

define host {
    use          linux-server
    host_name   machine-physique
    alias        machine physique
    address     192.168.1.30
    max_check_attempts 3
    check_period    24x7
    notification_interval 30
    notification_period 24x7
}

```

```

# sudo systemctl restart apache2
# sudo systemctl reload nagios

```

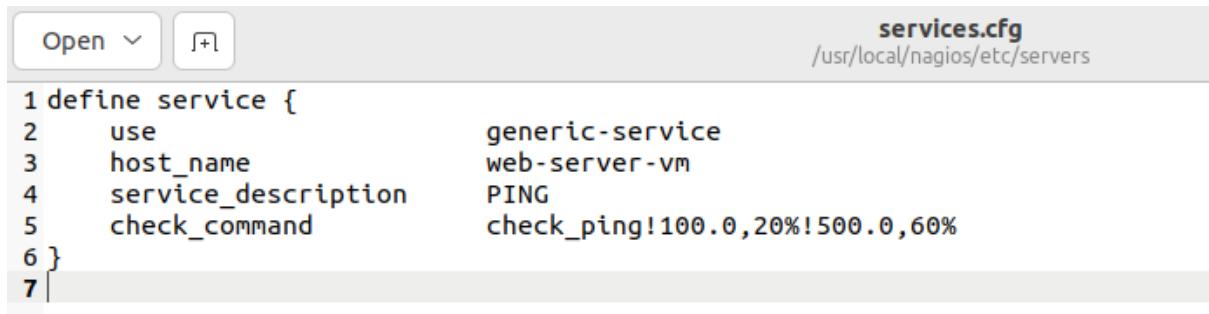
Click on hosts in the left pane to see hosts being monitored by Nagios.

The screenshot shows the Nagios web interface at localhost/nagios/. The top navigation bar includes links for Home, Documentation, and Current Status. The Current Status menu is expanded, showing options like Tactical Overview, Map (Legacy), Hosts, Services, Host Groups, Service Groups, and Problems. The main content area displays the "Host Status Details For All Host Groups" table, which lists three hosts: localhost, machine-physique, and web-server-vm, all in an UP status. Above the table, summary statistics are shown for Host Status Totals (Up: 3, Down: 0, Unreachable: 0, Pending: 0) and Service Status Totals (Ok: 7, Warning: 0, Unknown: 0, Critical: 1, Pending: 0).

Host	Status	Last Check	Duration	Status Information
localhost	UP	10-08-2023 13:47:34	0d 0h 59m 38s	PING OK - Packet loss = 0%, RTA = 0.10 ms
machine-physique	UP	10-08-2023 13:46:23	0d 0h 8m 58s	PING OK - Packet loss = 0%, RTA = 1.25 ms
web-server-vm	UP	10-08-2023 13:50:07	0d 0h 0m 14s	PING OK - Packet loss = 0%, RTA = 0.94 ms

You can monitor a specific service on a machine supervised by Nagios. To do so, you need to create a service definition in Nagios service configuration file /usr/local/nagios/etc/servers/services.cfg.

Here's an example configuration of a PING service in Nagios:

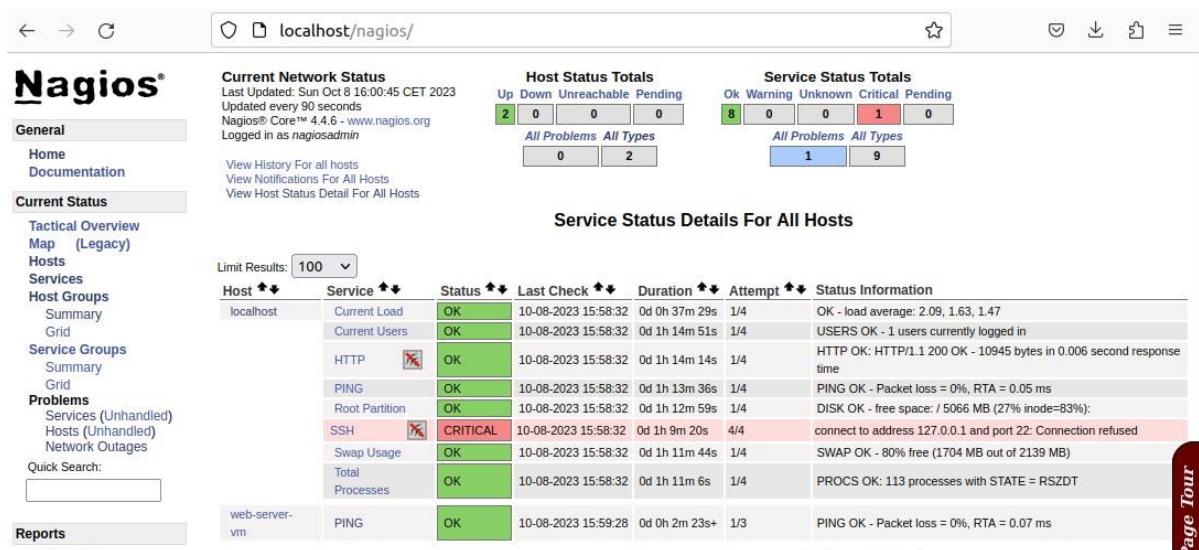


```

1 define service {
2     use generic-service
3     host_name web-server-vm
4     service_description PING
5     check_command check_ping!100.0,20%!500.0,60%
6 }
7

```

Click on services in the left pane to see services being monitored by Nagios.



Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	10-08-2023 15:58:32	0d 0h 37m 29s	1/4	OK - load average: 2.09, 1.63, 1.47
	Current Users	OK	10-08-2023 15:58:32	0d 1h 14m 51s	1/4	USERS OK - 1 users currently logged in
	HTTP	CRITICAL	10-08-2023 15:58:32	0d 1h 14m 14s	1/4	HTTP OK: HTTP/1.1 200 OK - 10945 bytes in 0.006 second response time
	PING	OK	10-08-2023 15:58:32	0d 1h 13m 36s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	Root Partition	OK	10-08-2023 15:58:32	0d 1h 12m 59s	1/4	DISK OK - free space: / 5066 MB (27% inode=83%):
	SSH	CRITICAL	10-08-2023 15:58:32	0d 1h 9m 20s	4/4	connect to address 127.0.0.1 and port 22: Connection refused
	Swap Usage	OK	10-08-2023 15:58:32	0d 1h 11m 44s	1/4	SWAP OK - 80% free (1704 MB out of 2139 MB)
	Total Processes	OK	10-08-2023 15:58:32	0d 1h 11m 6s	1/4	PROCS OK: 113 processes with STATE = RSZDT
web-server-vm	PING	OK	10-08-2023 15:59:28	0d 0h 2m 23s+	1/3	PING OK - Packet loss = 0%, RTA = 0.07 ms