Network Monitoring

- Monitoring the entire infrastructue
- Detecting of any network or server problems
- Finding the cause of any issues
- Maintaining security and availiability of service
- Monitoring performances or troubleshoot
- Responding automatically to any issues

Monitoring with Nagios

Nagios®

1. Installation

- Goto: https://www.nagios.com/downloads/nagios-xi/
- Choose your platform and install Nagios
- Install from sources (Recommended!)

core
https://www.nagios.org/downloads/nagios-core/thanks/?skip=1&product_download=nagioscore-source

Plugins
https://www.nagios.org/downloads/nagios-plugins/

Nagios in Ubuntu Linux

Security-Enhanced Linux

This guide is based on SELinux being disabled or in permissive mode. SELinux is not enabled by default on Ubuntu. If you would like to see if it is installed run the following command:

sudo dpkg -l selinux*

Prerequisites

Perform these steps to install the pre-requisite packages.

===== Ubuntu 14.x / 15.x =====
sudo apt-get update
sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2
apache2-utils php5 libgd2-xpm-dev

===== Ubuntu 16.x / 17.x =====
sudo apt-get update
sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2
php libapache2-mod-php7.0 libgd2-xpm-dev

===== Ubuntu 18.x =====
sudo apt-get update
sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2
php libapache2-mod-php7.2 libgd-dev

===== Ubuntu 20.x =====
sudo apt-get update
sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2
php libapache2-mod-php7.4 libgd-dev

sudo apt-get install openssl libssl-dev

Downloading the Source
cd /tmp
wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.6.tar.gz
tar xzf nagioscore.tar.gz

Compile

cd /tmp/nagioscore-nagios-4.4.6/
sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled
sudo make all

Create User And Group

This creates the nagios user and group. The www-data user is also added to the nagios group.

sudo make install-groups-users

sudo usermod -a -G nagios www-data

Install Binaries

This step installs the binary files, CGIs, and HTML files.

sudo make install

Install Service/Daemon

This installs the service or daemon files and also configures them to start on boot.

sudo make install-daemoninit

Information on starting and stopping services will be explained further on.

Install Command Mode

This installs and configures the external command file.

sudo make install-commandmode

Install Configuration Files

This installs the *SAMPLE* configuration files. These are required as Nagios needs some configuration files to allow it to start.

sudo make install-config

Install Apache Config Files

This installs the Apache web server configuration files and configures Apache settings.

sudo make install-webconf
sudo a2enmod rewrite
sudo a2enmod cgi

Configure Firewall

You need to allow port 80 inbound traffic on the local firewall so you can reach the Nagios Core web interface.

sudo ufw allow Apache
sudo ufw reload

Create nagiosadmin User Account

You'll need to create an Apache user account to be able to log into Nagios.

The following command will create a user account called nagiosadmin and you will be prompted to provide a password for the account.

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

When adding additional users in the future, you need to remove -c from

the above command otherwise it will replace the existing nagiosadmin user (and any other users you may have added).

Start Apache Web Server

===== Ubuntu 14.x =====

Need to restart it because it is already running.

sudo service apache2 restart

===== Ubuntu 15.x / 16.x / 17.x / 18.x / 20.x =====

Need to restart it because it is already running.

sudo systemctl restart apache2.service

Start Service/Daemon

This command starts Nagios Core.

===== Ubuntu 14.x =====

sudo start nagios

===== Ubuntu 15.x / 16.x / 17.x / 18.x / 20.x =====

sudo systemctl start nagios.service

Test Nagios

Nagios is now running, to confirm this you need to log into the Nagios Web Interface.

Point your web browser to the ip address or FQDN of your Nagios Core server, for example:

http://10.25.5.143/nagios

http://core-013.domain.local/nagios

You will be prompted for a username and password. The username is nagiosadmin (you created it in a previous step) and the password is what you provided earlier.

Once you have logged in you are presented with the Nagios interface. Congratulations you have installed Nagios Core.

BUT WAIT ...

Currently you have only installed the Nagios Core engine. You'll notice some errors under the hosts and services along the lines of:

(No output on stdout) stderr:
execvp(/usr/local/nagios/libexec/check_load, ...) failed. errno is 2:
No such file or directory

These errors will be resolved once you install the Nagios Plugins,

which is covered in the next step.

Installing The Nagios Plugins

Nagios Core needs plugins to operate properly. The following steps will walk you through installing Nagios Plugins.

These steps install nagios-plugins 2.4.3. Newer versions will become available in the future and you can use those in the following installation steps. Please see the releases page on GitHub for all available versions.

Please note that the following steps install most of the plugins that come in the Nagios Plugins package. However there are some plugins that require other libraries which are not included in those instructions. Please refer to the following KB article for detailed installation instructions:

Installing Nagios Plugins From Source

Prerequisites

Make sure that you have the following packages installed.

sudo apt-get install -y autoconf gcc libc6 libmcrypt-dev make libssl-dev wget bc gawk dc build-essential snmp libnet-snmp-perl gettext

Downloading The Source

cd /tmp
wget --no-check-certificate -O nagios-plugins.tar.gz https://github.com/nagios-plugins/nagios-plugins/archive/release-2.4.3.tar.gz
tar zxf nagios-plugins.tar.gz

Compile + Install

cd /tmp/nagios-plugins-release-2.4.3/
sudo ./tools/setup

sudo ./configure
sudo make
sudo make install

Test Plugins

Point your web browser to the ip address or FQDN of your Nagios Core server, for example:

http://10.25.5.143/nagios

http://core-013.domain.local/nagios

Go to a host or service object and "Re-schedule the next check" under the Commands menu. The error you previously saw should now disappear and the correct output will be shown on the screen.

Service / Daemon Commands

Different Linux distributions have different methods of starting / stopping / restarting / status Nagios.

===== Ubuntu 14.x =====

sudo start nagios
sudo stop nagios
sudo restart nagios
sudo status nagios

===== Ubuntu 15.x / 16.x / 17.x / 18.x / 20.x =====

sudo systemctl start nagios.service
sudo systemctl stop nagios.service
sudo systemctl restart nagios.service
sudo systemctl status nagios.service

2. Configuration files

- **nagios.cfg** The main configuration file of Nagios core. Contains the location of log file of Nagios, hosts and services state update interval, users and groupds, paths, etc.
- **cgi.cfg** data they might need. It contains all the user and group information and their rights and permissions.
- **resource.cfg** You can define $USERx$ macros which are useful for storing sensitive information such as usernames, passwords, etc.
- **commands.cfg** Provides command definitions. These commands are used to check and monitor hosts and services.
- **contacts.cfg** Contains contacts and groups information of Nagios. By default, one contact is already present Nagios admin.
- **templates.cfg** Provides some example object definition templates that are referred by other host, service, contact, etc.
- **timeperiods.cfg** Provides some example timeperiod definitions that you can refer in host, service, contact, and dependency definitions.

3. Continuous Monitoring

Continuous Monitoring is all about the ability of an organization to detect, report, respond, contain and mitigate the attacks that occur, in its infrastructure.

- It detects all the server and network problems.
- It finds the root cause of the failure.
- It helps in reducing the maintenance cost.
- It helps in troubleshooting the performance issues.
- It helps in updating infrastructure before it gets outdated.
- It can fix problems automatically when detected.
- It makes sure the servers, services, applications, network is always up and running.
- It monitors complete infrastructure every second.

4. Hosts and Services

Nagios is the most popular tool which is used to monitor hosts and services running in your IT infrastructure.

- Host is just like a computer; it can be a physical device or virtual.
- Services are those which are used by Nagios to check something about a host.

sudo nano /usr/local/nagios/etc/servers/ubuntu_host.cfg

```
define host {
    use linux-server
    host_name ubuntu_host
    alias Ubuntu Host
    address 192.168.1.10
    register 1
}
define service {
    host_name ubuntu_host
    service_description PING
    check_command check_ping!100.0,20%!500.0,60%
```

```
    max_check_attempts 2
    check_interval 2
    retry_interval 2
    check_period 24x7
    check_freshness 1
    contact_groups admins
    notification_interval 2
    notification_period 24x7
    notifications_enabled 1
    register 1
}
```

Debian live with persistence.

First try with official image from www.debian.org/CD/live/
From SE site (standard live):

wget -c https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/debian-live-11.6.0-amd64-xfce.iso

Then checksum you download file with

https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/SHA256SUMS

Ok ISO filesystem is read-only, but there is a little workaround: we could replace non vital bootparam by persistence in this way.

Once file validated !
you could alter them by using sed for replacing strings in binary.

LANG=C sed ’s/splash quiet/persistence /;s/quiet splash/persistence /’ <./debian-l

This will create a modified copy of your live binary file, by strictly replacing splash quiet or quiet splash by persistence, everywhere. Ok this will work only while grub boot command do contain this two words together.

But care to not miss the space after persistence:

"splash quiet" -> 12 characters
"persistence " -> 12 characters

Or your binary will be broken.

Install on USB key

dd if=debian-live-11.6.0-amd64-xfce-persist.iso of=/dev/sdX

Then add your third partition for persistence:

```
fdisk /dev/sdX
n               # new partition
p               # primary
<Return>        # default: 3
<Return>        # default: next free sector
<Return>        # default: last addressable sector
w               # write and quit
```

This could be run without interaction:

fdisk /dev/sdX <<<$'n\np\n\n\n\nw'

Format and prepare persistence with union:

```
mkfs.ext4 -L persistence /dev/sdX3
mount /dev/sdX3 /mnt
echo '/ union' >/mnt/persistence.conf
sync
umount /mnt
```

Then eject and try!

If you use official, unmodified image, for using persistence, you have to interrupt boot selection: Once menu screen is displayed, choose your boot option, then instead of Return, hit Tab. The kernel commandline will be displayed, then add persistence with a space, after last word (quiet), then hit Return. Unfortunately, as 1st partition is bundled with UEFI and is ISO, you can't modify the boot command.

Serial communication with Linux

- Very useful in data centers!
- Use an RS-232 serial and DB-9 serial cables.

- Find the serial port:
  $ dmesg |grep tty
- Very useful in data centers!

- Use an RS-232 serial and DB-9 serial cables.

- Find the serial port:
  ```
  $ dmesg |grep tty
  $ setserial -g /dev/ttyUSB[0123]
  $ ls /dev/serial/by-id/
  ```
- Connect the serial cable to the serial port
- Login with tio or minicom
  ```
  $ l -g /dev/ttyUSB[0123]
  $ ls /dev/serial/by-id/
  ```

- Connect the serial cable to the serial port
- Login with tio or minicom

```
$ tio /dev/ttyUSB0
```

Challenge no 3

Continuous Monitoring with Nagios

Q1. Install and configure Nagios.

Q2. What is Nagios?

Q3. How does Nagios works?

Q4. Explain Main configuration file and its location.

Q5. What are plugins in Nagios?

Q6. Describe the difference between active and passive check.

Q7. Explain Nagios state types.

Q8. What is Flapping in Nagios?

Q9. What is State Stalking in Nagios?