**Nagios**

As you browse sites for Nagios, there are only a few websites that have given information on this wonderful [monitoring tool](https://www.janbasktraining.com/blog/devops-tools/). So, I believe that this post would be a clear idea of what are Nagios, configuration, installation, and continuous monitoring with the Nagios. The tool keeps a close eye on your entire IT infrastructure, services, business processes, and the servers etc.

**What is Continuous Monitoring?**

Once the application is deployed to the server, the role of continuous monitoring comes into existence. The process is all about taking care of Company infrastructure and respond immediately as soon as some error occurs. The concept is not new but it is around for a long time.

The technique you must have heard about is the static analysis that is responsible to detect, respond or report the logs but the analysis is not so much accurate as expected by the organizations. With the Continuous monitoring, you can perform and respond each of the activities in the best possible way.

When we discuss the continuous monitoring, this is necessary that all pieces of information should be connected well like database, warehouse, security tools, security management system, AI, security intelligence, data analytics etc. Connecting different pieces together in a well-organized manner is the crux of the process that makes the continuous monitoring more successful and useful requirement by the organizations?

Further, the process is performed on the continuous (on-going) basis that reports immediately about the risks that can be faced by Company for its poor infrastructure. You can also check the behavior of networks and data analytics report when required. According to a saying, if you cannot ‘measure’ the risks how will you ‘manage’ them and continuous monitoring is the solution that works best here.

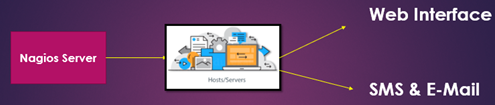
### ****Why is Continuous Monitoring useful?****

Continuous Monitoring has the capability to detect the system errors before they could have negative impacts on your business productivity. Here, is a quick list of features that explain to you why continuous monitoring is useful –

* The process helps in detecting network errors or server crashes.
* With CM, you can detect or report any type of infrastructure issues quickly.
* It also helps in maintaining security issues and service availability.
* You can troubleshoot or monitor the performance issues of the server.
* The process gives you a perfect idea of infrastructure upgrades, how can you make it even better that suits Company needs.
* The process has the capability of reporting issues at first glance only.
* The issues can be fixed automatically as soon as they are identified during the monitoring process.
* On successful completion of continuous monitoring, it makes sure that it does not have any negative impact on your Company infrastructure and business operations.
* The entire business process and IT infrastructure can be monitored in a single pass only.

## **What is Nagios?**

Nagios is useful for continuous monitoring of applications, servers, or business processes etc. [inside a DevOps](https://www.janbasktraining.com/blog/devops-tutorial/) culture. It gives information to the technical staff about any performance issues or drawbacks in the system. When you use Nagios, you don’t have to give much explanation how an unseen defect in the infrastructure can affect your organizational health badly.



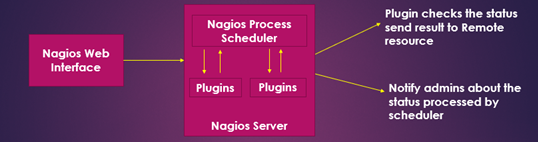
Consider the diagram given above to get a clear idea of Nagios working –

Nagios is running on a server where plug-ins is installed and running automatically. They further contact the hosts/servers on your network and give you the status message in two different forms – one is Web Interface and the other is SMS or E-mail.

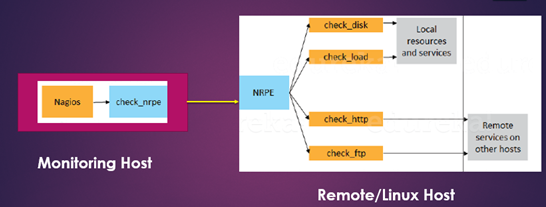
Further, Nagios Server as shown in the diagram earlier works as a scheduler and runs selected scripts after a repeated time interval. As soon as the requirement changes, the previous scripts will be stored and new scripts will run based on needs. In brief, Nagios working is based on Plug-ins that gives the confirm status of server, application, or infrastructure issues.

#### **Nagios Infrastructure**

The Nagios platform is based on the server-agent architecture. Take an example where Nagios is usually running over a host and plugins are designed to interact with the local network that should be monitored. Further, plug-ins send useful information to the scheduler that will be displayed over GUI.



You also need to understand the working of NRPE – Nagios Remote plug-in Executor. With the NRPE, the plug-ins are executed over local servers or Linux machines. The objective of NRPE is to closely monitor the local resources over a remote resource.



As per the rule, these resources should not be exposed to the external machines. This is the reason why NRPE is needed along with other important components. You can better understand the working of NRPE by looking at the diagram below –

* Check\_NRPE is a plugin that is available on local monitoring machine.
* The NRPE daemon runs over the remote machine or Linux server and further monitors the resources and services for local and other hosts.
* As you can see, there is one secure SSL connection between monitoring host and the remote/Linux host that is shown by the yellow arrow in the diagram.

Let us have some hands-on practice by this quick tutorial i.e. Nagios Installation and Configuration.

NRPE –> Nagios remote plugins executor that will interact with nagios plugins and provide data of client to nagios plugins. So, this will install toward nagios client machine. No need on nagios server side.

To access nagios via browser we need httpd package. And dashboard of nagios is deigned in php language. So let’s install all these prerequisite dependencies first.

## **Nagios Installation and Configuration Tutorial Guide**

#### **Step 1 – Pre-requisites**

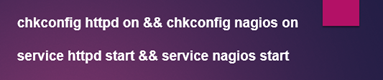
basic packages like gcc compiler, build essential, apache, php and root/sudo access.

#### **Step 2 – Installing Nagios, Nagios Plugins, and NRPE**

Execute the following command on the terminal to install, Nagios plug-ins and NRPE (Nagios Resource Plug-in Executor), Apache and PHP. Apache is needed to monitor the recent web server status and PHP is required to process the dynamic content on your website.

Nagios Tutorial Guide

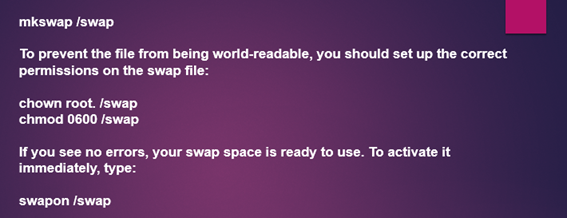
In the next step, you should enable the Apache server with ‘chkconfig’ command as shown below in the screenshot. And once it is enabled start the Nagios and the Apache server with the ‘service’ command given below.



Now create the swap file and avail minimum 1 GB space with the ‘dd’ command as given below –

Nagios Tutorial Guide

With the swap file, you can free up necessary space and shift it somewhere else to the hard drive. You can use “mkwsap” command to create the swap partitions and prepare the remote host for a swap area. The final command should be written like this as shown below –



With the above command, only a temporary swap file is created. You can make the swap area permanent by adding it to the fstab file. Nagios Tutorial Guide

With this command, we are done with the second step. Now let us move to the third step i.e. how to configure Nagios to access the Web interface.

#### **Step 3 – Configure Nagios to access the Web Interface**

At this step, you need to first set the password for web interface by typing the following command over terminal – Nagios Tutorial Guide

Retype the password to confirm it. Now open the web browser and type the local hostname in the address bar.  Here, you need to enter the username and the password that is just given by you. By default, the username is Nagios admin. You can change the username in the advanced settings option. Password would the same that we set earlier. In the end, press OK. It will show Nagios dashboard in front of you as shown below. With these steps, you can monitor localhost only. If you are interested in monitoring the remote host then you need to install the NRPE.

https://www.janbasktraining.com/blog/what-is-nagios/

Nagios offers following features making it usable by a large group of user community −

* It can monitor Database servers such as SQL Server, Oracle, Mysql, Postgres
* It gives application level information (Apache, Postfix, LDAP, Citrix etc.).
* Provides active development.
* Has excellent support form huge active community.
* Nagios runs on any operating system.
* It can ping to see if host is reachable.

## **Benefits of Nagios**

Nagios offers the following benefits for the users −

* It helps in getting rid of periodic testing.
* It detects split-second failures when the wrist strap is still in the “intermittent” stage.
* It reduces maintenance cost without sacrificing performance.
* It provides timely notification to the management of control and breakdown.

**Nagios contains various products as discussed in detail below −**

## **Nagios XI**

It provides monitoring for complete IT infrastructure components like applications, services, network, operating systems etc. It gives a complete view of your infrastructure and business processes. The GUI is easily customizable giving the used flexibility. The standard edition of this tool and enterprise edition costs.

## **Nagios Core**

It is the core on monitoring IT infrastructure. Nagios XI product is also fundamentally based on Nagios core. Whenever there is any issue of failure in the infrastructure, it sends an alert/notification to the admin who can take the action quickly to resolve the issue. This tool is absolutely free.

## **Nagios Log Server**

It makes searching of log data very simple and easy. It keeps all the log data at one location with high availability setup. It can easily send alerts if any issue is found in the log data. It can scale to 1000s of severs giving more power, speed, storage, and reliability to your log analysis platform. The price of this tool depends on the number of instances – i.e. from 1 Instance to 10 Instances.

## **Nagios Fusion**

This product provides a centralized view of complete monitoring system. With Nagios Fusion, you scan setup separate monitoring servers for separate geographies. It can be easily integrated with Nagios XI and Nagios core to give the complete visibility of the infrastructure. This tool costs.

## **Nagios Network Analyser**

It gives the complete information of the network infrastructure to the admin with the potential threats on the network so that admin can take quick actions. It shares very detailed data about the network after in-depth network analysis. This tool costs.

Nagios - Installation

Before you install Nagios, some packages such as Apache, PHP, building packages etc., are required to be present on your Ubuntu system. Hence, let us install them first.

**Step 1** − Run the following command to install pre-required packages −

yum install -y wget httpd php gcc glibc glibc-common gd gd-devel make net-snmp

libgd-dev sendmail unzip

**Step 2** − Next, create user and group for Nagios and add them to Apache www-data user.

Sudo useradd nagios

sudo groupadd nagcmd

sudo usermod -a -G nagcmd nagios

sudo usermod -a -G nagios,nagcmd www-data

**Step 3** − Download the latest Nagios package.

cd /home/ec2-user/

wget https://sourceforge.net/projects/nagios/files/nagios-4.x/nagios-4.2.1/nagios-4.2.1.tar.gz

**Step 4** − Extract the tarball file.

tar -xzf nagios-4.2.1.tar.gz

cd nagios-4.2.1/

**Step 5** − Run the following command to compile Nagios from source.

./configure --with-nagios-group=nagios --with-command-group=nagcmd

**Step 6** − Run the following command to build Nagios files.

make all

**Step 7** − Run the command shown below to install all the Nagios files.

sudo make install

**Step 8** − Run the following commands to install init and external command configuration files.

sudo make install-commandmode

sudo make install-init

sudo make install-config

sudo make install-webconf

sudo /usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sitesavailable/

nagios.conf

**Step 9** − Now copy the event handler directory to Nagios directory.

sudo cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/

sudo chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers

// TO VERIFY THE NAGIOS CONFIGURATION

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

//START THE NAGIOS AND APACHE

service nagios start

service httpd start

//TO PROTECT NAGIOS WEBSITE PLEASE CREATE A USERNAME AND PASSWORD

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

password admin

user nagiosadmin

**Step 10** − Download and extract Nagios plugins.

cd

wget https://nagios-plugins.org/download/nagios-plugins-2.1.3.tar.gz

tar -xzf nagios-plugins-2.1.3.tar.gz

cd nagios-plugins-2.1.3/

**Step 11** − Install Nagios plugins using the below command.

./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl

make

sudo make install

**Step 12** − Now edit the Nagios configuration file and uncomment line number 51 → cfg\_dir=/usr/local/nagios/etc/servers

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

**Step 13** − Now, create a server directory.

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

**Step 14** − Edit contacts configuration file.

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

service nagios start

**Step 15** − Now enable the Apache modules and configure a user nagiosadmin.

sudo a2enmod rewrite

sudo a2enmod cgi

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

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

**Step 16** − Now, restart Apache and Nagios.

service apache2 restart

service nagios start

cd /etc/init.d/

sudo cp /etc/init.d/skeleton /etc/init.d/Nagios

**Step 17** − Edit the Nagios file.

sudo gedit /etc/init.d/Nagios

DESC = "Nagios"

NAME = nagios

DAEMON = /usr/local/nagios/bin/$NAME

DAEMON\_ARGS = "-d /usr/local/nagios/etc/nagios.cfg"

PIDFILE = /usr/local/nagios/var/$NAME.lock

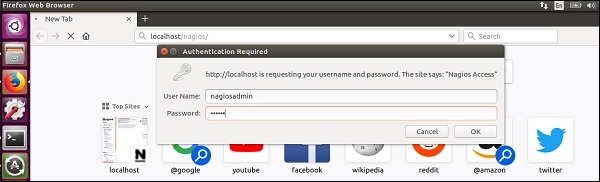
**Step 18** − Make the Nagios file executable and start Nagios.

sudo chmod +x /etc/init.d/nagios

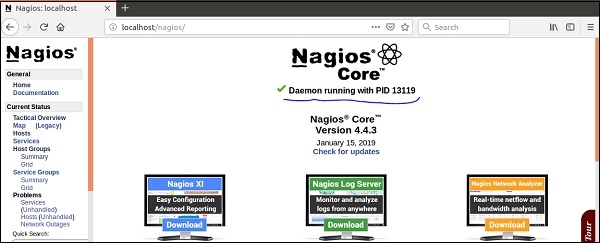
service apache2 restart

service nagios start

**Step 19** − Now go to your browser and open url → **http://localhost/nagios**. Now login to Nagios with username nagiosadmin and use the password which you had set earlier. The login screen of Nagios is as shown in the screenshot given below −



If you have followed all the steps correctly, you Nagios web interface will show up. You can find the Nagios dashboard as shown below −



Add new Hosts

* whereis Nagios
* cd /usr/local/Nagios/etc/objects
* Modify/Add emailID && group
* vi contacts.cfg

define contact{

contact\_name nagiosadmin ; Short name of user

use generic-contact ; Inherit default values from generic-contact template

alias Nagios Admin ; Full name of user

email nagios@localhost ; <<\*\*\*\*\* CHANGE THIS TO YOUR EMAIL ADDRESS \*\*\*\*\*\*

}

* define contactgroup{

contactgroup\_name admins

alias Nagios Administrators

members nagiosadmin

}

* Add servers
  + vi localhost.cfg

define host{

use linux-server ; Name of host template to use

; This host definition will inherit all variables that are defined

; in (or inherited by) the linux-server host template definition.

host\_name webserver

alias webserver

address 127.0.0.1

}

define service{

use local-service ; Name of service template to use

host\_name localhost, webserver

service\_description PING

check\_command check\_ping!100.0,20%!500.0,60%

}

* service nagios reload -> to load the changes
* cd /var/www/html

add the html file

* Change the time period
  + vi timeperiods.cfg

Add remote server

* create another instance of ec2 machine
* install httpd and tomcat
* copy the ipaddress of the ec2 instance
* Add client IP address and hostname
  + vi localhost.cfg

define host{

use linux-server ; Name of host template to use

; This host definition will inherit all variables that are defined

; in (or inherited by) the linux-server host template definition.

host\_name remoteserver

alias remoteserver

address 13.127.21.131

}

* + define service{

use local-service ; Name of service template to use

host\_name localhost, webserver, remoteserver

service\_description PING

check\_command check\_ping!100.0,20%!500.0,60%

}

* service nagios reload -> to load the changes

Add New Plugin

* Get the tomcat plugin
* cd /usr/local/nagios/libexec
* curl "https://exchange.nagios.org/components/com\_mtree/attachment.php?link\_id=2522&cf\_id=24" -o check\_tomcat.pl
* mv check\_tomcat.pl check\_tomcat
* chmod +x /usr/local/nagios/libexec/check\_tomcat
* ./check\_tomcat -h
* /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
* chown nagios:nagios /usr/local/nagios/libexec/check\_tomcat
* Configure the tomcat plugin
* cd /usr/local/Nagios/etc/objects
* vi commands.cfg

# 'check\_tomcat' command definition

define command{

command\_name check\_tomcat

command\_line $USER1$/check\_tomcat -H $HOSTADDRESS$ -p $ARG1$ -l $ARG2$ -a $ARG3$ -w $ARG4$ -c $ARG5$

}

* vi localhost.cfg:

# Define a service to check the state of a Tomcat service

define service{

use local-service

host\_name localhost

service\_description Tomcat

check\_command check\_tomcat!8080!tomcat!tomcat!25%,25%!10%,10%

}

* service nagios reload

<https://www.tutorialspoint.com/nagios/index.htm>

<https://www.tutorialspoint.com/articles/how-to-configure-nagios-server-for-monitoring-apache-server>

https://www.linuxtopic.com/2017/06/nagios-add-remote-host-centos-7.html

Interview question of nagios configuration and installation

 1.What is RTA value 20% means in nagios?

 2.What is nagios template file?

 3.What is nagios home directory?

 4.What is extension of nagios file?

  5.How many service state are available nagios?

Ans :- There are mainly four state of service in nagios.

OK, Warning, Critical, Unknown

 6.How many default attempt nagios use to check any service status?

 7.After how much time nagios will send alert. Tell the set default value.

 8.How to monitor cloud infra from local nagios server?

 9.What is configuration file of nagios server?

 10.What is port number of nagios server?

 Answer care fully.

   11.What is soft state and hard state in nagios?

Ans :- To change service from one state to another state means let’s take a scenario to understand better suppose 30% cpu load is going on your server then this is in OK state . If suddenly increase cpu 30% more then it became total 60% and you have set your  warning value at 50% cpu utilization. So, state has been changed from ok to warning or you can say stat has been changed from soft state to hard stat. This process is called soft and hard state.

   12.what is active and passive checks in nagios?

Ans When Nagios server gather the information  from client mean nagios server will reach to client and request for data static. This is called active check. But in case of passive check client will provide data matrix to nagios server.

 13.what is active alarm and passive alarm?

 14.what is communication protocol of nagios?

<https://exchange.nagios.org/directory/Tutorials/Other-Tutorials-And-HOWTOs/Step-By-Step-Install-&-Configure-Nagios/details>

https://sysadminxpert.com/how-to-add-linux-host-to-nagios-monitoring-server/