Aim: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

Steps:

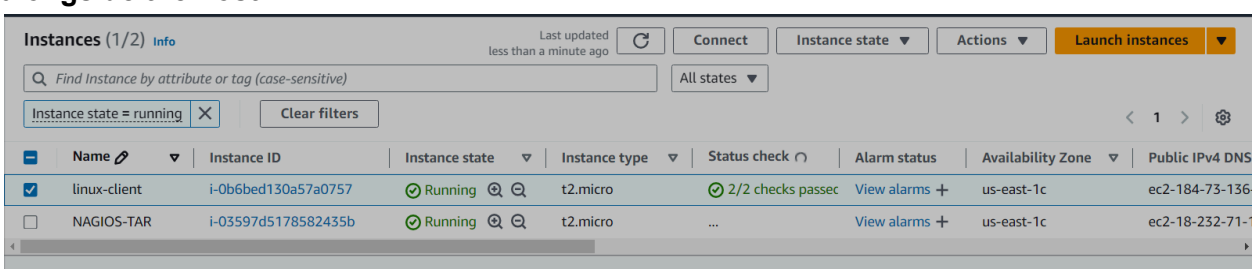
Prerequisites: AWS Free Tier, Nagios Server running on Amazon Linux Machine.

1. To Confirm that Nagios is running on the server side, run this sudo systemctl status nagios on the “NAGIOS HOST”.

```
Last login: Thu Oct 10 08:58:32 2024 from 18.206.107.27
[ec2-user@ip-172-31-39-132 ~]$ sudo systemctl status nagios
● nagios.service - Nagios Core 4.4.6
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Sun 2024-10-13 11:51:57 UTC; 16min ago
       Docs: https://www.nagios.org/documentation
    Process: 1993 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/>
    Process: 1995 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUC>
   Main PID: 1997 (nagios)
      Tasks: 6 (limit: 1112)
     Memory: 2.7M
        CPU: 150ms
     CGroup: /system.slice/nagios.service
             ├─1997 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─1998 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─1999 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─2000 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─2001 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─2007 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 13 11:51:57 ip-172-31-39-132.ec2.internal nagios[1997]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfull>
Oct 13 11:51:57 ip-172-31-39-132.ec2.internal nagios[1997]: qh: core query handler registered
Oct 13 11:51:57 ip-172-31-39-132.ec2.internal nagios[1997]: qh: echo service query handler registered
Oct 13 11:51:57 ip-172-31-39-132.ec2.internal nagios[1997]: qh: help for the query handler registered
Oct 13 11:51:57 ip-172-31-39-132.ec2.internal nagios[1997]: wproc: Successfully registered manager as @wproc with query>
Oct 13 11:51:57 ip-172-31-39-132.ec2.internal nagios[1997]: wproc: Registry request: name=Core Worker 2000;pid=2000
Oct 13 11:51:57 ip-172-31-39-132.ec2.internal nagios[1997]: wproc: Registry request: name=Core Worker 2001;pid=2001
Oct 13 11:51:57 ip-172-31-39-132.ec2.internal nagios[1997]: wproc: Registry request: name=Core Worker 1999;pid=1999
```

2. Before we begin,
To monitor a Linux machine, create an Ubuntu 20.04 server EC2 Instance in AWS.Provide it with the same security group as the Nagios Host and name it ‘linux-client’ alongside the host.



3. On the server, run this command

ps -ef | grep nagios

```
[ec2-user@ip-172-31-39-132 ~]$ ps -ef | grep nagios
nagios      1997       1  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios      1998    1997  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagio
s.qh
nagios      1999    1997  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagio
s.qh
nagios      2000    1997  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagio
s.qh
nagios      2001    1997  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagio
s.qh
nagios      2007    1997  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user    3125    2836  0 12:15 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-39-132 ~]$
```

4. Become a root user and create 2 folders
sudo su
mkdir /usr/local/nagios/etc/objects/monitorhosts
mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts

5. Copy the sample localhost.cfg file to linuxhost folder
cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

6. Open linuxserver.cfg using nano and make the following changes
nano
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
Change the hostname to linuxserver (EVERYWHERE ON THE FILE)
Change address to the public IP address of your LINUX CLIENT.

```
root@ip-172-31-39-132:/home
  GNU nano 5.8              /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
###############################################################################



###############################################################################
#
# HOST DEFINITION
#
###############################################################################

# Define a host for the local machine

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               linuxserver
    alias                   localhost
    address                 184.73.136.82
}



###############################################################################
#

^G Help      ^O Write Out   ^W Where Is    ^K Cut       ^T Execute    ^C Location   M-U Undo     M-A Set Mark
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify    ^/ Go To Line M-E Redo     M-6 Copy
```

```
define hostgroup {

    hostgroup_name          linux-servers1          ; The name of the hostgroup
    alias                   Linux Servers           ; Long name of the group
    members                 localhost               ; Comma separated list of hosts that belong to this group
}
```

7. Open the Nagios Config file and add the following line
nano /usr/local/nagios/etc/nagios.cfg
##Add this line
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/

```
# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

#cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc/switches
#cfg_dir=/usr/local/nagios/etc/routers
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/



# OBJECT CACHE FILE
# This option determines where object definitions are cached when
# Nagios starts/restarts.  The CGIs read object definitions from
```

8. Verify the configuration files
9. Restart the nagios service

service nagios restart

10. Make a package index update and install gcc, nagios-nrpe-server and the plugins.

sudo apt update -y

sudo apt install gcc -y

sudo apt install -y nagios-nrpe-server nagios-plugins

11. Open nrpe.cfg file to make changes.

sudo nano /etc/nagios/nrpe.cfg

Under allowed_hosts, add your nagios host IP address like so

12. Restart the NRPE server

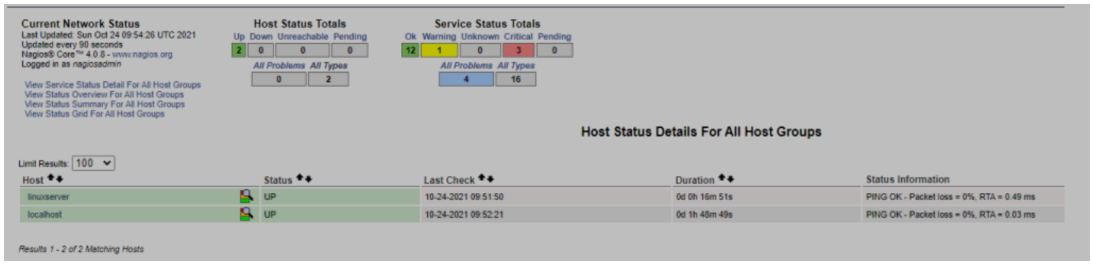
sudo systemctl restart nagios-nrpe-server

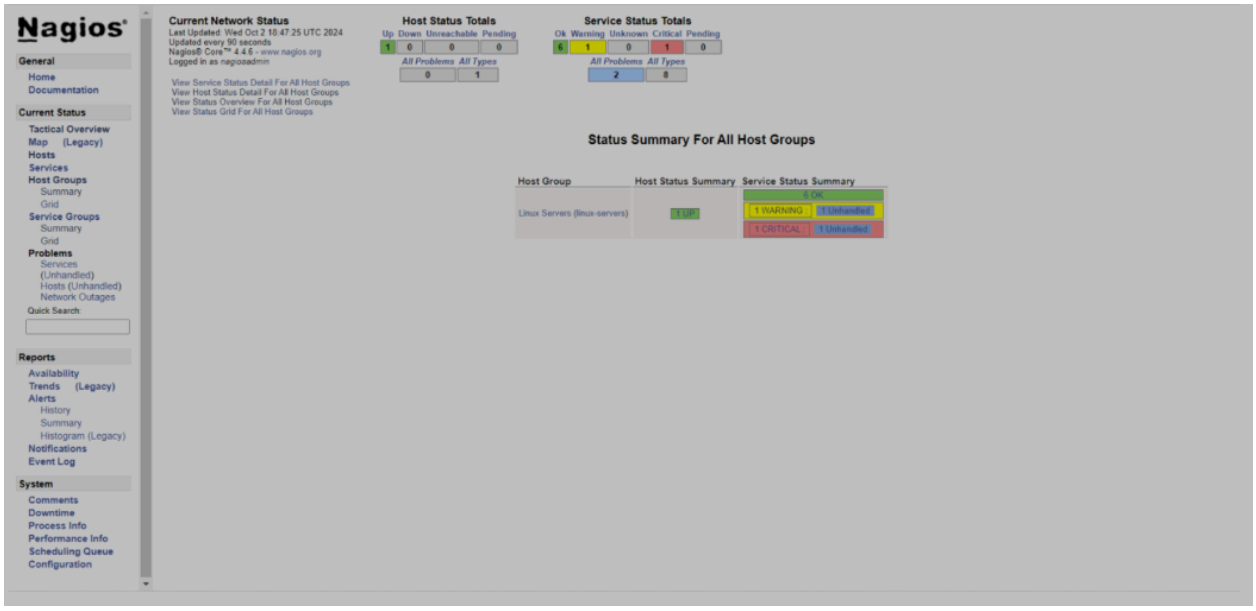
```
# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address.  I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd



allowed_hosts=127.0.0.1, 13.232.100.28
```

13. Now, check your nagios dashboard and you'll see a new host being added.





Conclusion:

Thus, we learned about service monitoring using Nagios and successfully monitored a Linux

Server and monitored its different ports and services using Nagios and NRPE.