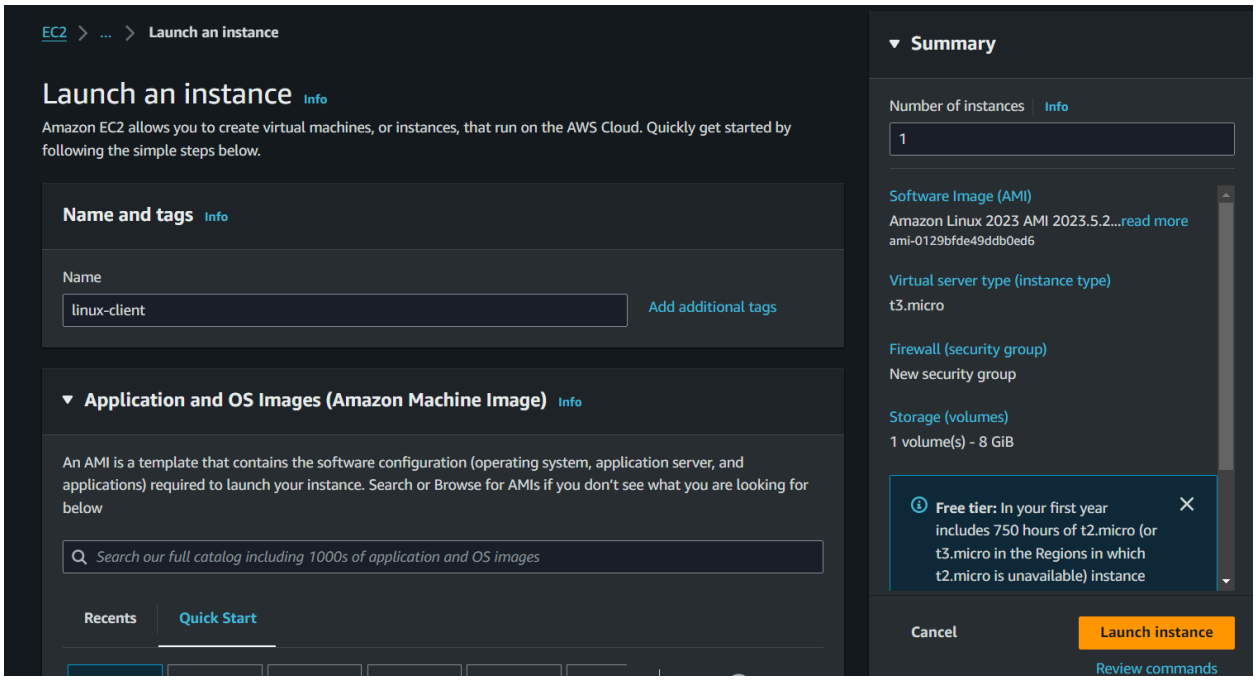
Experiment 10

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

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

Step 1: Create a new ec2 instance called linux-client and choose Ubuntu as operating system.



Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents | Quick Start

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Li

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible

ami-04cdc91e49cb06165 (64-bit (x86)) / ami-02b7539372433cf6b (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

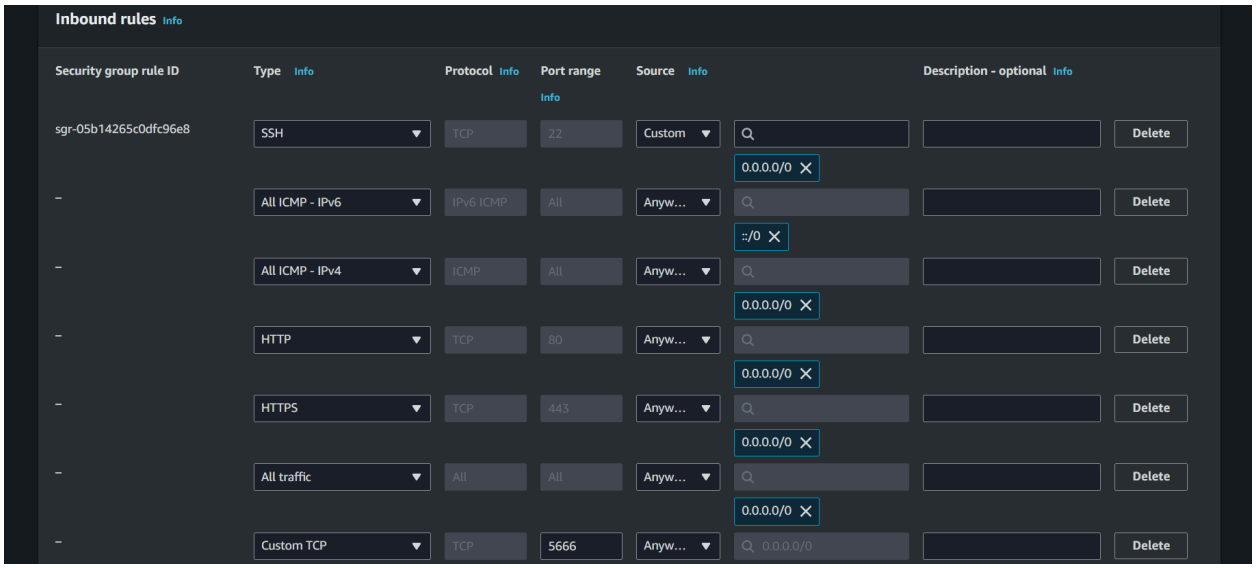
EC2 > ... > Launch an instance

Success

Successfully initiated launch of instance (i-0f2dd6bd87339d15e)

Launch log

Step 2: Change the settings for security groups



Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-05b14265c0dfc96e8	SSH	TCP	22	Custom	0.0.0.0/0		Delete
-	All ICMP - IPv6	IPv6 ICMP	All	Anyw...	::/0		Delete
-	All ICMP - IPv4	ICMP	All	Anyw...	0.0.0.0/0		Delete
-	HTTP	TCP	80	Anyw...	0.0.0.0/0		Delete
-	HTTPS	TCP	443	Anyw...	0.0.0.0/0		Delete
-	All traffic	All	All	Anyw...	0.0.0.0/0		Delete
-	Custom TCP	TCP	5666	Anyw...	0.0.0.0/0		Delete

On server, check if server is running then, ps -ef | grep nagios

```
[ec2-user@ip-172-31-38-129 ~]$ ps -ef | grep nagios
nagios      1628       1  0 07:20 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios      1633    1628  0 07:20 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      1634    1628  0 07:20 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      1635    1628  0 07:20 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      1636    1628  0 07:20 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      1637    1628  0 07:20 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user   34154   33992  0 09:19 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-38-129 ~]$
```

Step 3: Copy Sample Configuration File

cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

Step 4: Edit the Configuration File

sudo nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

- Change hostname to linuxserver everywhere in the file.
- Change address to the public IP address of your linux-client.

```
###############################################################################
#
# 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                   linuxserver
    address                 13.60.19.89
}



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

```
  GNU nano 5.8                    /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
# HOST GROUP DEFINITION
#
###############################################################################

# Define an optional hostgroup for Linux machines

define hostgroup {

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



###############################################################################
#
# SERVICE DEFINITIONS
#
###############################################################################

# Define a service to "ping" the local machine

define service {

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

Step 5: Update Nagios Configuration
sudo nano /usr/local/nagios/etc/nagios.cfg

- Add the following line:

cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/

```
  GNU nano 5.8                                                    /usr/local/nagios/etc/nagios.cf
# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg


# 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
```

Step 6: Verify Configuration Files
sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

```
[root@ip-172-31-38-129 ec2-user]# nano /usr/local/nagios/etc/nagios.cfg
[root@ip-172-31-38-129 ec2-user]# sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.4.6
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2020-04-28
License: GPL

Website: https://www.nagios.org
Reading configuration data...
   Read main config file okay...
   Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
        Checked 16 services.
        Checked 2 hosts.
        Checked 2 host groups.
        Checked 0 service groups.
        Checked 1 contacts.
        Checked 1 contact groups.
        Checked 24 commands.
        Checked 5 time periods.
        Checked 0 host escalations.
```

In client side:

Step 9: Update Package Index and Install Required Packages

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

Step 10: Edit NRPE Configuration File

sudo nano /etc/nagios/nrpe.cfg

- Add your Nagios host IP address under allowed_hosts:

allowed_hosts=<Nagios_Host_IP>

```
# 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,::1,16.171.175.50



# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed.  This option only works
# if the daemon was configured with the --enable-command-args configure script
```

Step 11: Restart NRPE Server
sudo systemctl restart nagios-nrpe-server

```
Restarting services...

Service restarts being deferred:
 /etc/needrestart/restart.d/dbus.service
 systemctl restart getty@tty1.service
 systemctl restart networkd-dispatcher.service
 systemctl restart serial-getty@ttyS0.service
 systemctl restart systemd-logind.service
 systemctl restart unattended-upgrades.service

No containers need to be restarted.

User sessions running outdated binaries:
 ubuntu @ session #2: sshd[1046,1498]
 ubuntu @ user manager service: systemd[1393]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-46-222:~$ sudo nano /etc/nagios/nrpe.cfg
ubuntu@ip-172-31-46-222:~$ sudo systemctl restart nagios-nrpe-server
ubuntu@ip-172-31-46-222:~$
```

Step 12: Check Nagios Dashboard

- Open your browser and navigate to http://<Nagios_Host_IP>/nagios.
- Log in with nagiosadmin and the password you set earlier.
- You should see the new host linuxserver added.
- Click on Hosts to see the host details.
- Click on Services to see all services and ports being monitored