

Experiment 10

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

Step 1: Initially confirm that Nagios is running on the server side. For this run the following command -
`sudo systemctl status nagios`
on the nagios-host instance.

```
[root@ip-172-31-93-157 nagios-plugins-2.0.31]# sudo systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
   Loaded: loaded (/etc/rc.d/init.d/nagios; generated)
   Active: active (running) since Mon 2024-09-30 18:02:27 UTC; 42s ago
     Docs: man:systemd-sysv-generator(8).
   Process: 79969 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
    Tasks: 6 (limit: 1112)
   Memory: 2.2M
      CPU: 52ms
   CGroup: /system.slice/nagios.service
           └─80009 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             └─80011 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─80012 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─80013 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─80014 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─80037 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Successfully registered manager as @wproc with query handler
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80011:pid=80011
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80014:pid=80014
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80013:pid=80013
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80012:pid=80012
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: Successfully launched command file worker with pid 80037
lines 1-26/26 (END)
```

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

Step 2: Once confirmed, make another instance with the same security group as that of nagios-host.
For now, leave this machine as it is, and go back to your nagios-host machine.

The screenshot displays the AWS Management Console interface for a Security Group. The left sidebar shows the navigation menu with categories like EC2 Dashboard, Instances, Images, Elastic Block Store, and Network & Security. The main content area shows the details for the Security Group 'launch-wizard-14'.

Security Group Details:

- Security group name:** launch-wizard-14
- Security group ID:** sg-0455135daa934e321
- Description:** launch-wizard-14 created 2024-09-30T18:26:54.458Z
- VPC ID:** vpc-0ec7dea564d6f7acf
- Owner:** 856746069793
- Inbound rules count:** 7 Permission entries
- Outbound rules count:** 1 Permission entry

Inbound rules (7):

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sg-r-01439baf13aca75fa	IPv6	All ICMP - IPv6	IPv6 ICMP	All
-	sg-r-07d8ce2ac9f5e6a92	IPv4	All traffic	All	All
-	sg-r-071fd6724622dd2...	IPv4	HTTPS	TCP	443
-	sg-r-0e47c6681768287...	IPv4	SSH	TCP	22
-	sg-r-0f594249495210d...	IPv4	Custom TCP	TCP	5666
-	sg-r-07b7ba4fe03f14614	IPv4	HTTP	TCP	80
-	sg-r-0fcb4849f80ee0409	IPv4	All ICMP - IPv4	ICMP	All

Step 3: Now run the following command -
`ps -ef | grep nagios`

```
Active: active (running) since Mon 2024-09-30 18:02:27 UTC; 42s ago
Docs: nagios systemd-sysv-generator(8)
Process: 79969 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
Tasks: 6 (limit: 1112)
Memory: 2.2M
CPU: 52ms
CGroup: /system.slice/nagios.service
└─0009 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
└─0011 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
└─0012 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
└─0013 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
└─0014 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
└─0037 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Successfully registered manager as @wproc with query handler
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80011;pid=80011
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80014;pid=80014
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80013;pid=80013
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: wproc: Registry request: name=Core Worker 80012;pid=80012
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please use the check_interval attribute instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use the retry_interval attribute instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please use the check_interval attribute instead.
Sep 30 18:02:27 ip-172-31-93-157.ec2.internal nagios[80009]: Successfully launched command file worker with pid 80037

[root@ip-172-31-93-157 nagios-plugins-2.0.3]# ps -ef | grep nagios
nagios      80009      1  0 18:02 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios      80011      80009  0 18:02 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      80012      80009  0 18:02 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      80013      80009  0 18:02 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      80014      80009  0 18:02 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      80037      80009  0 18:02 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
root        81960     3110  0 18:35 pts/1    00:00:00 grep --color=auto nagios

[root@ip-172-31-93-157 nagios-plugins-2.0.3]#
```

Step 4: Now, run the following commands -

```
sudo su
mkdir /usr/local/nagios/etc/objects/monitorhosts
mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

```
root@ip-172-31-93-157 nagios-plugins-2.0.3]# sudo su
root@ip-172-31-93-157 nagios-plugins-2.0.3]# mkdir /usr/local/nagios/etc/objects/monitorhosts
root@ip-172-31-93-157 nagios-plugins-2.0.3]# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
root@ip-172-31-93-157 nagios-plugins-2.0.3]# cp /usr/local/nagios/etc/objects/localhost.cfg
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
cp: missing destination file operand after '/usr/local/nagios/etc/objects/localhost.cfg'
try 'cp --help' for more information.
bash: /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg: No such file or directory
root@ip-172-31-93-157 nagios-plugins-2.0.3]# nano
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
bash: /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg: No such file or directory
root@ip-172-31-93-157 nagios-plugins-2.0.3]# cp /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
cp: missing destination file operand after '/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg'
try 'cp --help' for more information.
root@ip-172-31-93-157 nagios-plugins-2.0.3]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
root@ip-172-31-93-157 nagios-plugins-2.0.3]#
```

Step 5: Open linuxserver.cfg using the the following command -

```
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.

Change hostgroup_name under hostgroup to linux-servers1

```
GNU nano 5.8 /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg Modified
# Example of how you can create configuration entries to monitor
# the local (Linux) machine.
#
#####

# 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          linux-server
    alias              linux-server
    address            3.95.202.23
}

#####

Help      Write Out  Where Is  Cut       Execute   Location  M-U Undo  M-R Set Mark  M-I To Bracket  M-O Previous
Exit     Read File  Replace  Paste    Justify   Go To Line M-E Redo  M-G Copy  M-Q Where Was M-W Next

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
```

```
GNU nano 5.8 /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg Modified
check_command          check_local_swap!20!10
}

# Define a service to check SSH on the local machine.
# Disable notifications for this service by default, as not all users may have SSH enabled.

define service{
    use                local-service      ; Name of service template to use
    host_name          linuxserver
    service_description SSH
    check_command       check_ssh
    notifications_enabled 0
}

# Define a service to check HTTP on the local machine.
# Disable notifications for this service by default, as not all users may have HTTP enabled.

define service{
    use                local-service      ; Name of service template to use
    host_name          linuxserver
    service_description HTTP
    check_command       check_http
    notifications_enabled 0
}

Help      Write Out  Where Is  Cut       Execute   Location  M-U Undo  M-R Set Mark  M-I To Bracket  M-O Previous
Exit     Read File  Replace  Paste    Justify   Go To Line M-E Redo  M-G Copy  M-Q Where Was M-W Next

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
```

Step 6: Open Nagios config file and add the following line -
nano /usr/local/nagios/etc/nagios.cfg

Then add this line -
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/

```
GNU nano 5.8 /usr/local/nagios/etc/nagios.cfg Modified
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# 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/[]

Help Write Out Where Is Cut Execute Location Undo Set Mark To Bracket Previous
Exit Read File Replace Paste Justify Go To Line Redo Copy Where Was Next

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
```

Step 8: Verify configuration files using the following command -
`sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg`

If there are no errors, run the following command -
`sudo service nagios start`

```
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# nano /usr/local/nagios/etc/nagios.cfg
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# nano /usr/local/nagios/etc/nagios.cfg
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# /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...
WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please use check_interval instead.
WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
WARNING: The normal_check_interval attribute is deprecated and will be removed in future versions. Please use check_interval instead.
WARNING: The retry_check_interval attribute is deprecated and will be removed in future versions. Please use retry_interval instead.
Error: Could not find any host matching "linuxserver" (config file '/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg', starting on line 45)
Error: Could not expand members specified in hostgroup (config file '/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg', starting on line 45)
Error processing object config files!

***> One or more problems was encountered while processing the config files...

Check your configuration file(s) to ensure that they contain valid
directives and data definitions.  If you are upgrading from a previous
version of Nagios, you should be aware that some variables/definitions
may have been removed or modified in this version.  Make sure to read
the HTML documentation regarding the config files, as well as the
'Whats New' section to find out what has changed.

[root@ip-172-31-93-157 nagios-plugins-2.0.3]# []

i-025f1d18f7c8a8cda (nagios-host)
PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
```

```
[root@ip-172-31-93-157 nagios-plugins-2.0.3]# service nagios restart
Restarting nagios (via systemctl):
[ OK ]
[root@ip-172-31-93-157 nagios-plugins-2.0.3]#
```

i-025f1d18f7c8a8cda (nagios-host)

PublicIPs: 3.86.198.73 PrivateIPs: 172.31.93.157

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

Step 9: After entering the correct credentials, you will see this page.

EC2 DashboardEC2 Global ViewEventsConsole-to-Code Preview

InstancesInstancesTypesLaunch TemplatesSpot RequestsSavings PlansReserved InstancesDedicated HostsCapacity Reservations

ImagesAMIsAMI Catalog

Elastic Block StoreVolumesSnapshotsLifecycle Manager

Network & SecuritySecurity GroupsElastic IPs

Instances (1/1) info

Last updated about 1 hour ago

ConnectInstance stateActionsLaunch instances

Find instance by attribute or tag (case-sensitive)

All states

Instance state = runningClear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
nagios-host	i-025f1d18f7c8a8cda	Running	t2.micro	2/2 checks passed	View alarms	us-east-1c	ec2-3-86-198-73.compute-1.amazonaws.com

i-025f1d18f7c8a8cda (nagios-host)

DetailsStatus and alarmsMonitoringSecurityNetworkingStorageTags

Instance summary info

Instance IDi-025f1d18f7c8a8cda (nagios-host)

IPv6 address-

Hostname typeIP name: ip-172-31-93-157.ec2.internal

Answer private resource DNS name-

Public IPv4 address copied3.86.198.73 | open address

Instance stateRunning

Private IP DNS name (IPv4 only)ip-172-31-93-157.ec2.internal

Instance typet2.micro

Private IPv4 addresses172.31.93.157

Public IPv4 DNSec2-3-86-198-73.compute-1.amazonaws.com | open address

Elastic IP addresses-

CloudShellFeedback© 2024, Amazon Web Services, Inc. or its affiliates. PrivacyTermsCookie preferences

←↻⚠ Not secure3.86.198.73/nagios/☆🔍📄🏠🔒🔧⋮🌐

Nagios®

General

Home

Documentation

Current Status

Tactical Overview

Map (Legacy)

Hosts

Services

Host Groups

Summary

Grid

Service Groups

Summary

Grid

Problems

Services (Unhandled)

Hosts (Unhandled)

Network Outages

Quick Search:

Reports

Availability

Trends (Legacy)

Alerts

History

Summary

Histogram (Legacy)

Notifications

Event Log

System

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Configuration

Current Network Status

Last Updated: Mon Sep 30 19:13:49 UTC 2024

Updated every 90 seconds

Nagios® Core™ 4.4.6 - www.nagios.org

Logged in as nagiosadmin

View Service Status Detail For All Host Groups

View Status Overview For All Host Groups

View Status Summary For All Host Groups

View Status Grid For All Host Groups

Host Status Totals

UpDownUnreachablePending

2000

All ProblemsAll Types

02

Service Status Totals

OKWarningUnknownCriticalPending

610048

All ProblemsAll Types

216

Host Status Details For All Host Groups

Limit Results:100▼

Host	Status	Last Check	Duration	Status Information
insanserver	UP	09-30-2024 19:13:16	0d 0h 0m 33s+	PING OK - Packet loss = 0%, RTA = 1.82 ms
localhost	UP	09-30-2024 19:01:49	0d 1h 11m 22s	PING OK - Packet loss = 0%, RTA = 0.04 ms

Results 1 - 2 of 2 Matching Hosts

Page Tour