

Module 11: Continuous Monitoring Using Nagios

Demo Document

edureka!

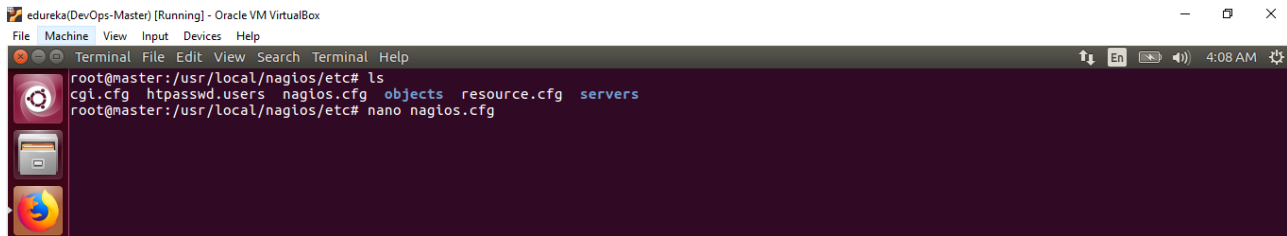
edureka!

© Brain4ce Education Solutions Pvt. Ltd.

Demo -1: Monitor the windows host using Nagios

Step 1: Check for the Nagios Directory.

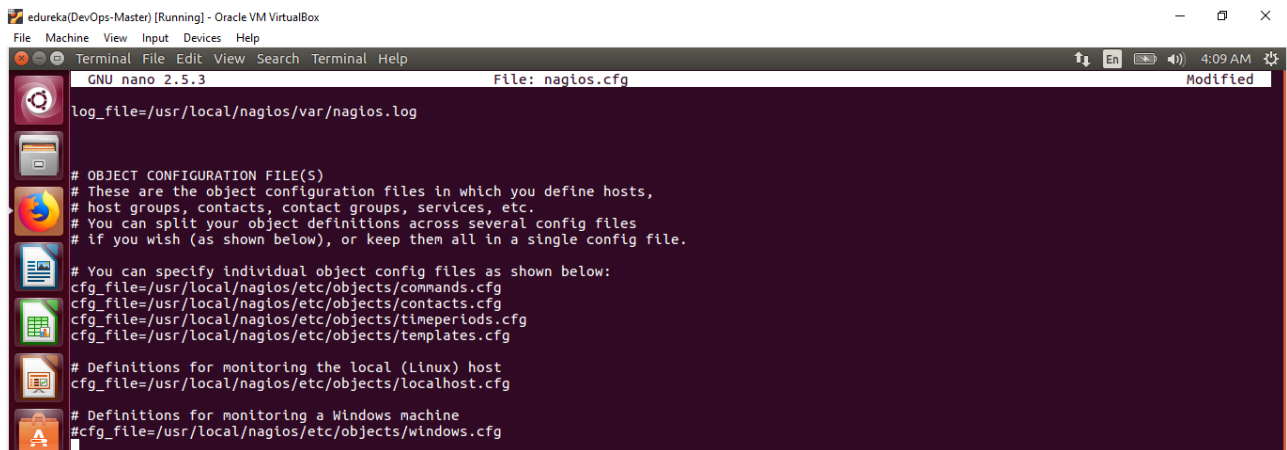
```
$cd /usr/local/nagios/etc
```



```
edureka(DevOps-Master) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
root@master:/usr/local/nagios/etc# ls
cgi.cfg  htpasswd.users  nagios.cfg  objects  resource.cfg  servers
root@master:/usr/local/nagios/etc# nano nagios.cfg
```

Step 2: Open nagios.cfg file

```
$nano nagios.cfg
```



```
edureka(DevOps-Master) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.5.3 File: nagios.cfg Modified
log_file=/usr/local/nagios/var/nagios.log

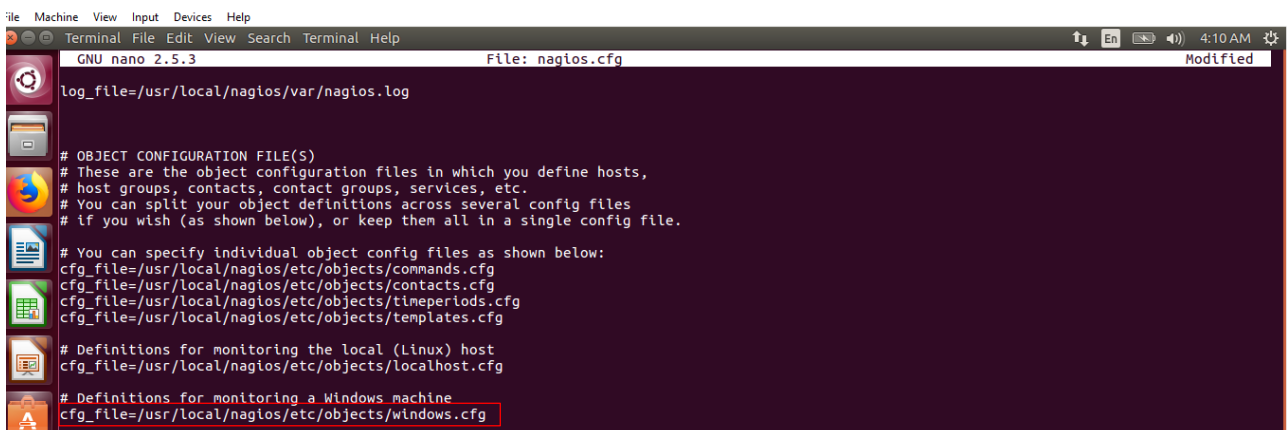
# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
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
```

Step 3: Remove the # sign for monitoring a windows machine.



```
edureka(DevOps-Master) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.5.3 File: nagios.cfg Modified
log_file=/usr/local/nagios/var/nagios.log

# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

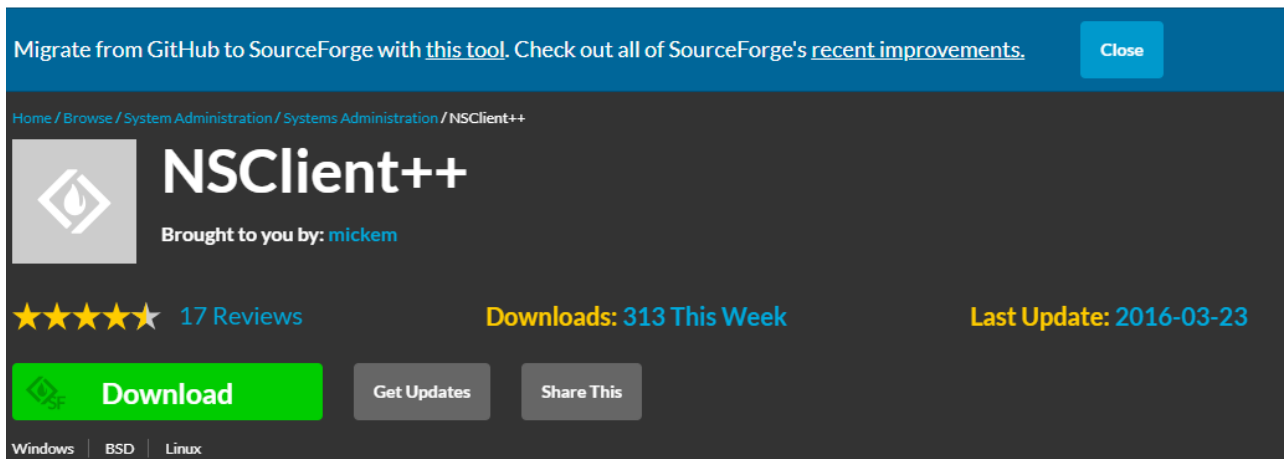
# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# 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
```

Step 4: Go to your windows machine and install NSClient++ plugin. Below given is the link to download that plugin.

<https://sourceforge.net/projects/nscplus/>



Click on Download button. After downloading, install it.

Step 5: Go to command line and use the below command to find the IP address of the machine and the host name as well.

```
$ipconfig /ALL
```

```
C:\Users\shubham>ipconfig /ALL

Windows IP Configuration

Host Name . . . . . : DESKTOP-38ICBQG
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix . :  
Description . . . . . : Intel(R) Dual Band Wireless-AC 3168  
Physical Address. . . . . : F4-96-34-68-5C-1D  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::3d2f:b284:692c:542%20(Preferred)  
IPv4 Address. . . . . : 192.168.1.25(Preferred)  
Subnet Mask . . . . . : 255.255.252.0  
Lease Obtained. . . . . : 18 July 2018 10:16:44  
Lease Expires . . . . . : 19 July 2018 10:31:39  
Default Gateway . . . . . : 192.168.1.1  
DHCP Server . . . . . : 192.168.1.1  
DHCPv6 IAID . . . . . : 167024180  
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-CD-16-1C-80-CE-62-36-8A-FC  
DNS Servers . . . . . : 192.168.1.1  
NetBIOS over Tcpip. . . . . : Enabled
```

Step 6: While defining a service, rename the hostname as mentioned in your windows machine for all the defined services. Replace all the host_name with your windows machine host_name. Also replace the address with IP address of windows machine.

```
define host{  
    use                windows-server ; Inherit default values from a template  
    host_name          DESKTOP-38ICBQG ; The name we're giving to this host  
    alias              My Windows Server ; A longer name associated with the host  
    address            192.168.2.69 ; IP address of the host  
}
```

```
define hostgroup{  
    hostgroup_name     windows-servers ; The name of the hostgroup  
    alias              Windows Servers ; Long name of the group  
}
```

```
# Create a service for monitoring the version of NSClient++ that is installed
# Change the host_name to match the name of the host you defined above

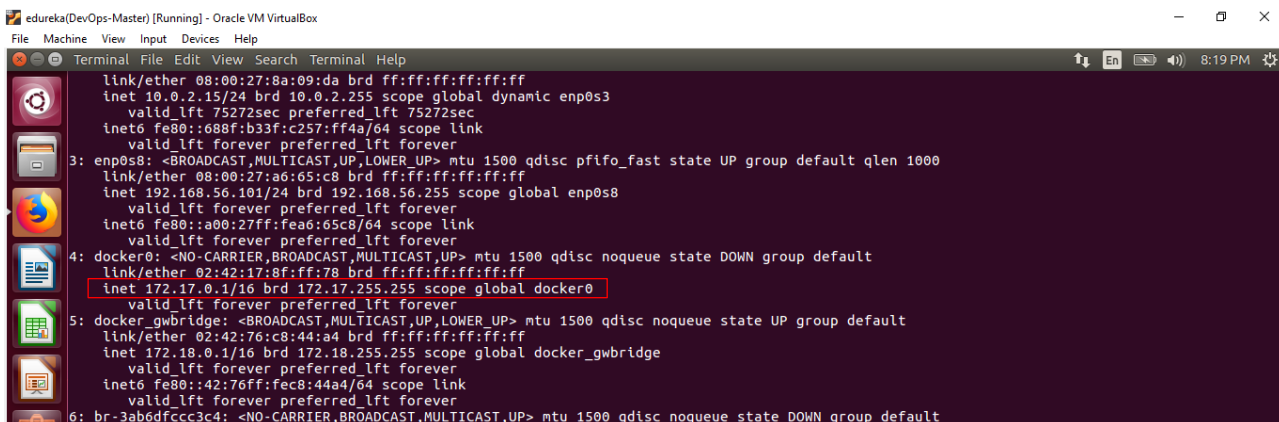
define service{
    use                generic-service
    host_name           DESKTOP-38ICBQG
    service_description NSClient++ Version
    check_command        check_nt!CLIENTVERSION
}
```

```
# Create a service for monitoring the Explorer.exe process
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name           DESKTOP-38ICBQG
    service_description Explorer
    check_command        check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
}
```

Step 7: Use the below command to identify the address on which Nagios is running:

```
$ip addr show
$service nagios start
$service apche2 start
```



```
edureka(DevOps-Master) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
link/ether 08:00:27:8a:09:da brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
    valid_lft 75272sec preferred_lft 75272sec
inet6 fe80::688f:b33f:c257:ff4a/64 scope link
    valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:a6:65:c8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea6:65c8/64 scope link
        valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:17:8f:ff:78 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
5: docker_gwbridge: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:76:c8:44:a4 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global docker_gwbridge
        valid_lft forever preferred_lft forever
    inet6 fe80::42:76ff:fec8:44a4/64 scope link
        valid_lft forever preferred_lft forever
6: br-3ab6dfccc3c4: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
```

Step 6: Go to browser and open Nagios Dashboard in the browser.

```
172.17.0.1/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

Current Network Status

Last Updated: Thu Mar 22 13:18:37 IST 2018
Updated every 90 seconds
Nagios® Core™ 4.2.0 - 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

Up	Down	Unreachable	Pending
2	0	0	0

All Problems: 0, All Types: 2

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
7	0	0	8	0

All Problems: 8, All Types: 15

Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
DESKTOP-38ICBQG	UP	03-22-2018 13:15:58	0d 0h 52m 32s	PING OK - Packet loss = 0%, RTA = 1.27 ms
localhost	UP	03-22-2018 13:15:43	0d 2h 9m 2s	PING OK - Packet loss = 0%, RTA = 0.14 ms

Results 1 - 2 of 2 Matching Hosts

Now, you can monitor your host and services running.

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

Current Network Status

Last Updated: Thu Mar 22 15:48:36 IST 2018
Updated every 90 seconds
Nagios® Core™ 4.2.0 - www.nagios.org
Logged in as nagiosadmin

View History for all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems: 0, All Types: 2

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
7	0	0	8	0

All Problems: 8, All Types: 15

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
DESKTOP-38ICBQG	C:\ Drive Space	CRITICAL	03-22-2018 15:41:56	0d 2h 10m 39s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	CPU Load	CRITICAL	03-22-2018 15:42:56	0d 2h 9m 40s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	Explorer	CRITICAL	03-22-2018 15:43:55	0d 2h 8m 41s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	Memory Usage	CRITICAL	03-22-2018 15:44:53	0d 2h 7m 43s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	NSClient++ Version	CRITICAL	03-22-2018 15:45:52	0d 2h 6m 44s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	Uptime	CRITICAL	03-22-2018 15:46:51	0d 2h 5m 45s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
localhost	W3SVC	CRITICAL	03-22-2018 15:47:49	0d 2h 4m 47s	3/3	connect to address 192.168.2.69 and port 12489: Connection refused
	Current Load	OK	03-22-2018 15:46:27	0d 3h 27m 9s	1/4	OK - load average: 0.50, 0.52, 0.50
	Current Users	OK	03-22-2018 15:47:05	0d 3h 26m 31s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	03-22-2018 15:47:42	0d 3h 25m 54s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0.003 second response time
	PING	OK	03-22-2018 15:48:20	0d 3h 25m 16s	1/4	PING OK - Packet loss = 0%, RTA = 0.09 ms
	Root Partition	OK	03-22-2018 15:43:57	0d 3h 24m 39s	1/4	DISK OK - free space: / 9557 MB (55% inode=78%):
	SSH	CRITICAL	03-22-2018 15:47:35	0d 3h 24m 1s	4/4	connect to address 127.0.0.1 and port 22: Connection refused
	Swap Usage	OK	03-22-2018 15:45:11	0d 3h 23m 24s	1/4	SWAP OK - 58% free (1180 MB out of 2045 MB)
localhost	Total Processes	OK	03-22-2018 15:45:50	0d 3h 22m 46s	1/4	PROCS OK: 55 processes with STATE = RSZDT

Results 1 - 15 of 15 Matching Services