FINAL REPORT:

Configuring Nagios to manage Servers

Group No - 13

Team Members

Dhrubodeep Basumatary(B16017)

Kaustubh Verma (B16021)

Randheer Kumar(B16139)

Akul Gupta (B16006)

Table of Contents :

1. Problem statement:

Managing a set of servers through nagios : It includes monitoring performance and availability of the servers .In case of failure of any service, Nagios attempt to correct the problem that caused the failure and then to automatically restart the service.

2. Introduction :

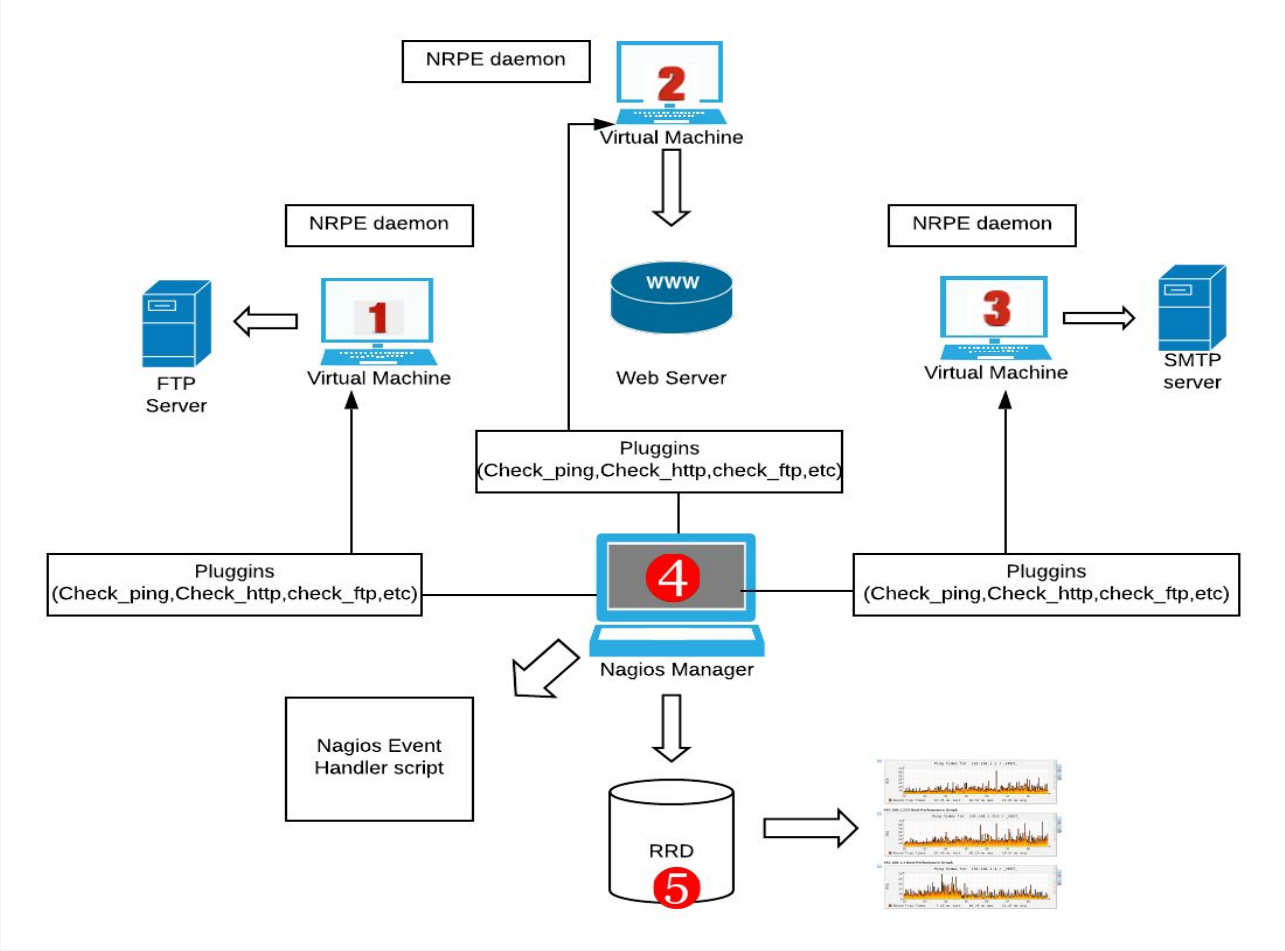
In this globalizing world, with new technology and tools emerging every now and then, it has become challenging to monitor their functioning and prevent them from having negative impact on product it is intended for. So to counter this, Nagios provides a continuous monitoring and alerting mechanism to ensure proper working of the servers, application and services.
Nagios is built on a client server architecture. Nagios plugins allows it to monitor the remote host machines.The Nagios server usually runs on a host and plugins run
on the remote hosts which needs to be monitored.
Nagios can also be used monitor via remotely run scripts via Nagios Remote Plugin Executor(NRPE).

There are 3 components of Nagios which are:

1. **Scheduler** : This is the server part of Nagios which is used to check the plugins and send notification according to the result.
2. **GUI** : This is the web interface of Nagios which displays web pages generated by CGI.
3. **Plugins:** Plugins are used to check a service and return the result to Nagios server. It can be configured by the user.

3. Overall Architecture:

Our design of Nagios works on servers installed in Virtual machines on different PC's,with Nagios installed on one of the PC's that is used to monitor and manage servers using event handler.The overall picture of design overview can be seen in the below diagram.



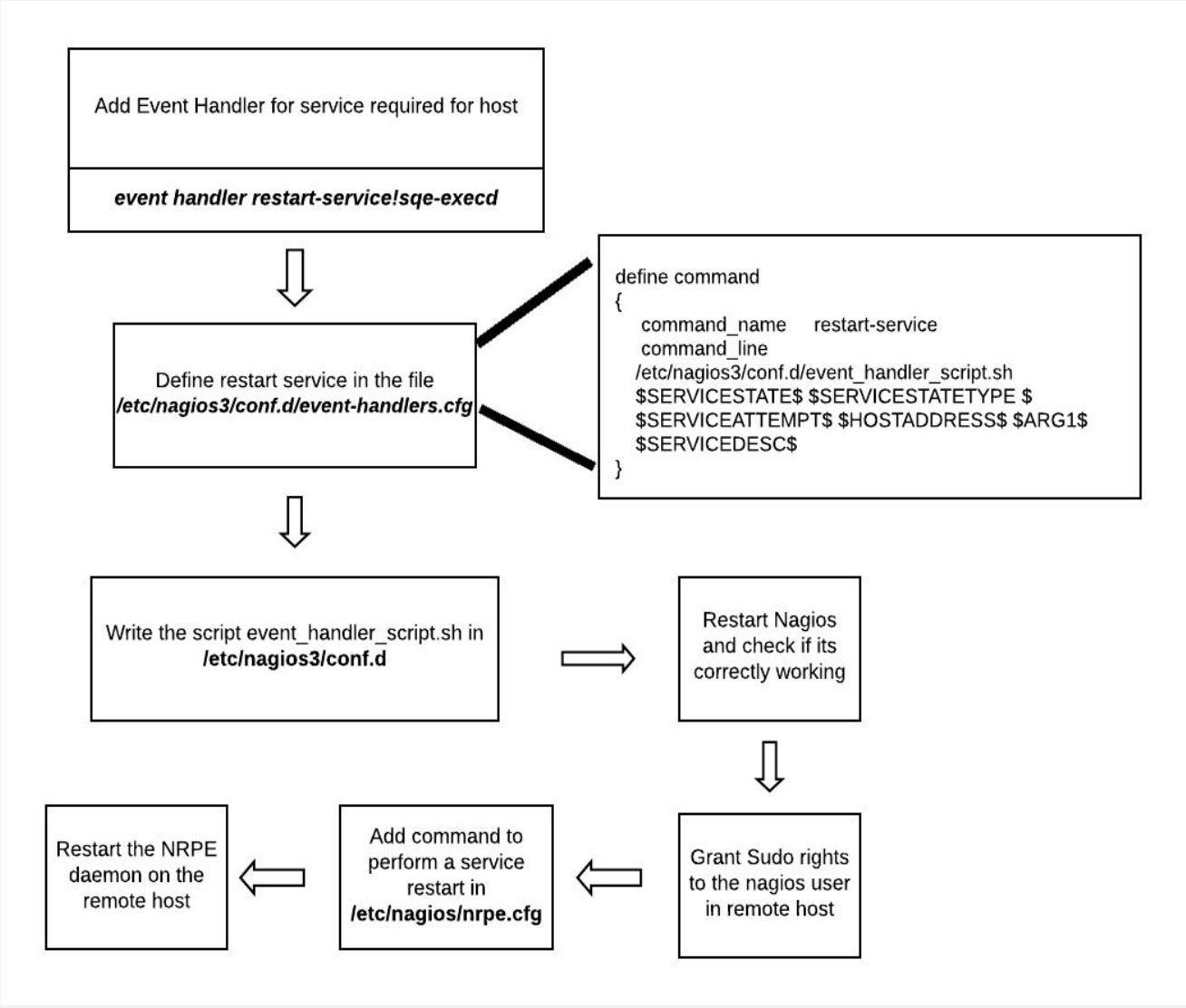
1. **Virtual Machine 1** : The Virtual Machine 1 runs the FTP server , FTP stands for file transfer protocol which is being used to transfer and exchange files between computers on a network . This machine contains SNMP daemons and NRPE plugins for being monitored by Nagios Manager.
2. **Virtual Machine 2**:The Virtual Machine 2 runs the web server which hosts websites . This machine also contains SNMP daemons and NRPE plugins for being monitored by Nagios Manager.
3. **Virtual Machine 3**:The Virtual Machine 2 runs the SMTP server , SMTP is acronym for simple mail transfer protocol used for sending email between servers.This machine contains SNMP daemons and NRPE plugins for being monitored by Nagios Manager.
4. **Nagios Manager** :The Nagios Manager monitors the three virtual machines that is connected to it and contains the event handler that can restart the applications services and devices if problems are detected.It contains the SNMP and CHECK_NRPE scripts . It monitors the machines for services like ping etc.

5. **RRD:** RRD stands for Round Robin database which stores the performance data generated by the nagios plugins . This data is extracted in graph using pnp4.

4. Design of Event Handler :

Detailed design of our architecture is shown in form of overall design overview as shown in previous figure and then the block diagrams of nagios event handler and tree based design making diagram of an example of an event handler script.

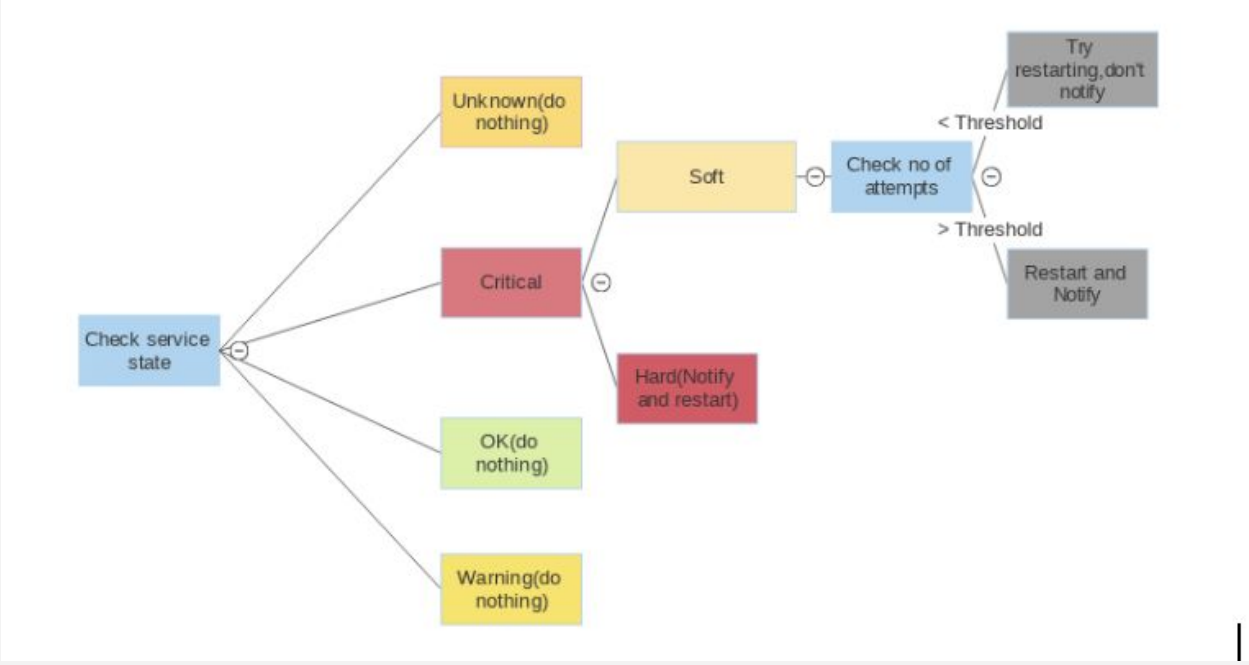
4.1 Nagios Event Handler(with NRPE)



For a basic event handler which restarts the service in case of failure, define the service in the config file of the server. Also define the restart command in commands.cfg file which links to a script. Hence

write the event handler script which is generally a shell script. If admin rights are required anywhere, grant that sudo rights to the Nagios.
Now restart the Nagios and check if the service is working correctly. For remote server, add command in nrpe and restart it to check whether the service starts running correctly or not.

4.2 Event Handler Script Example



Above decision making tree diagram shows an example of event handler script that makes the decisions on the basis of the states of the service it receives.

Checking service states :
There are 4 possible states -

1. Ok: Service is working fine. In this state we do nothing.
2. Critical: It means service is not working. In this state we restart the server through script .
3. Unknown: Either service is in working or not working.(so don't make any decisions).
4. Warning: Service is working but It can go in critical state or ok state after some time.

5. List of Components:

Servers - Web server, FTP server ,SMTP server.
The above mentioned three servers are set up on three virtual machines on three different PC's.

Nagios - interface with SNMP and NRPE. One of the PC's has nagios installed with SNMP and NRPE to monitor other servers and runs event handler script on the server to restart the server or perform other operation.

NRPE daemon on the servers.
Servers have NRPE daemon which enables them to perform operation according to the script.

Nagios Event Handler setup.
Nagios Event Handler enables the task to run script that performs according to the states received from the servers.

Services to monitor :SSH,ping , Cpu load,Ram usage,User CPU usage ,etc.
Above mentioned are the services that would be monitored on the servers.

Configuring nagios to send notifications(when needed).
This feature can be added to the nagios services which can send notifications whenever needed.

6. Interfaces

The interface includes the webserver ,smtp server and ftp server on different machines, monitored with Nagios on one PC that monitors and runs event handlers. Remote hosts are monitored with the help of nrpe.

7. Algorithms and Data Structure

There are no significant algorithms for our project except a basic nrpe script written in shell that makes decisions based on the states of the server.

8. Setup configurations

Web server setup :

For setting up the web server we performed the following steps :

Step1:

```
# sudo apt-get update
# sudo apt-get install apache2
# sudo apt install mysql-server
# sudo apt install php7.0 libapache2-mod-php7.0 php7.0-mysql
```

We then hosted our html page and examined our machine from the nagios manager machine.

After setting up web server we perform the following steps for installing the Nrpe daemon.

NRPE DAEMON SETUP:

Remote Host Setup.

Step2:

i) We firstly install the Nagios plugins

```
# wget http://nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gzLa
# tar xzf nagios-plugins-2.2.1.tar.gz
# cd nagios-plugins-2.2.1
```

`-We then` Compile and install the plugins.

```
#./configure
# make
# make install
```

Depending on the version of the plugins, the permissions on the plugin directory and the plugin may need to be fixed at this point. If so run the following commands:

```
# useradd nagios
# groupadd nagios
# usermod -a -G nagios nagios
# chown nagios.nagios /usr/local/nagios
```

```
# chown -R nagios.nagios /usr/local/nagios/libexec
```

We then install the nrpe daemon for our machine

```
# wget
https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-3.2.1/
e-3.2.1.tar.gz
#tar xzf nrpe-3.2.1.tar
#cd nrpe-nrpe-3.2.1
```

Compile the NRPE addon:

```
# ./configure
# make all
# make install
# make install-config
# make install-inetd
# systemctl enable nrpe && systemctl start nrpe
```

After that we test the NRPE daemon locally , it's time to see if things are working properly make sure if the nrpe daemon is running :

```
# netstat -at | egrep "nrpe|5666"tcp00 *:nrpe*:*LISTEN
```

If the line above shows up then our nrpe daemon is working.
The sample command definitions run some of the plugins that were installed in step . However we edited the command definitions, added new commands, etc, by editing the NRPE config file :

```
# nano /usr/local/nagios/etc/nrpe.cfg
```

We added the following line in the command header ,this command was triggered whenever the nagios manger used the event handler to restart the webserver.

```
# command[restart-http]=/usr/bin/sudo /etc/init.d/apache2 start
```

FTP server setup :

Step 1: Installing VsFTP Server

```
# sudo apt-get install vsftpd
```

Step 2 : Start the FTP server and make it to start automatically from the next system Boot

```
# service vsftpd start
# chkconfig --level 35 vsftpd on
```

Step 3 : open ports 21 and 20 where the FTP daemons are listening

```
# sudo ufw allow 20/tcp
# sudo ufw allow 21/tcp
```

Step 4: Configuring and Securing VsFTP

Open file : `$ sudo nano /etc/vsftpd.conf`

Add few lines to specify values as anonymous_enable=NO,tcp_wrappers=YES,etc.

Step 5: Add user to allow ftp service in vsftpd.userlist :

Adding user:

```
# sudo useradd -m -c"Kaustubh" -s /bin/bash Kaustubh
# sudo passwd Kaustubh

# sudo nano /etc/vsftpd.userlist.
```

Set userlist_deny=NO which ensures only specific user can login.

Add user Kaustubh in userlist.

```
# echo "Kaustubh" | sudo tee -a /etc/vsftpd.userlist.
```

SMTP server setup :

Step 1: install postfix

```
# sudo DEBIAN_PRIORITY=low apt install postfix
```

Step 2 : Tweak the Postfix Configuration

```
# sudo postconf -e 'home_mailbox= Maildir/'
# sudo postconf -e 'virtual_alias_maps=
hash:/etc/postfix/virtual'
```

Step 3 : Map Mail Addresses to Linux Accounts:

```
# sudo nano /etc/postfix/virtual
```

admin@example.com user1
b16139@students.iitmandi.ac.in user1
b16017@students.iitmandi.ac.in user1

```
# sudo postmap /etc/postfix/virtual
# sudo systemctl restart postfix
```

Step 4 :Setting up the Environment to Match the Mail Location:

```
# echo 'export MAIL=~/Maildir' | sudo tee -a /etc/bash.bashrc | sudo
tee -a /etc/profile.d/mail.sh
# source /etc/profile.d/mail.sh
```

Step 5 : Install and Configure the Mail Client

```
# sudo apt install s-nail
```

We then follow the nrpe installation process described in the setup of our web server above for ftp and smtp also.

9. Visual Demo:

Intial Nagios interface when http server(monitor_http) and ftp server(monitor_ftp).

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Users	OK	05-22-2019 17:32:13	44d 21h 17m 42s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	05-22-2019 17:29:15	1d 17h 26m 8s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0.001 second response time
	PING	OK	05-22-2019 17:29:15	22d 19h 36m 15s	1/4	PING OK - Packet loss = 0%, RTA = 0.08 ms
	RAM	OK	05-22-2019 17:29:15	0d 17h 28m 30s	1/4	OK - 2621 / 7874 MB (33%) Free Memory, Used: 2797 MB, Shared: 476 MB, Buffers + Cached: 2454 MB
	Remote Load	OK	05-22-2019 17:32:13	0d 2h 13m 15s	1/4	OK - load average: 0.47, 0.52, 0.68
proftpserver	PING	OK	05-22-2019 17:31:55	0d 0h 0m 25s	1/4	PING OK - Packet loss = 0%, RTA = 80.95 ms
	Remote Load	OK	05-22-2019 17:31:17	0d 0h 49m 18s	1/4	SNMP OK - Average:
	monitor ftp	OK	05-22-2019 17:31:50	0d 0h 2m 30s	1/4	FTP OK - 0.005 second response time on localhost port 21 [220 (vsFTPd 3.0.3)]
students.iitmandi.ac.in	PING	WARNING	05-22-2019 17:27:15	0d 0h 5m 5s	4/4	PING WARNING - Packet loss = 0%, RTA = 116.02 ms
	Remote Load	OK	05-22-2019 17:30:53	0d 0h 49m 18s	1/4	SNMP OK - Average:
webbserver	PING	WARNING	05-22-2019 17:32:03	0d 0h 31m 6s	4/4	PING WARNING - DUPLICATES FOUND! Packet loss = 0%, RTA = 98.44 ms
	Remote Load	OK	05-22-2019 17:31:16	0d 0h 49m 18s	1/4	SNMP OK - Average:
	monitor http	OK	05-22-2019 17:31:16	0d 0h 30m 5s	1/4	HTTP OK: HTTP/1.1 200 OK - 11192 bytes in 0.001 second response time

Results 1 - 13 of 13 Matching Services

Stopped FTP server

```
my_ubuntu@my_ubuntu:~$ sudo service vsftpd stop
my_ubuntu@my_ubuntu:~$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
   Active: inactive (dead) since Wed 2019-05-22 13:13:46 UTC; 3s ago
  Process: 2806 ExecStart=/usr/sbin/vsftpd /etc/vsftpd.conf (code=killed, signal
  Process: 2799 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, s
 Main PID: 2806 (code=killed, signal=TERM)

May 22 13:13:27 my_ubuntu systemd[1]: Starting vsftpd FTP server...
May 22 13:13:27 my_ubuntu systemd[1]: Started vsftpd FTP server.
May 22 13:13:46 my_ubuntu systemd[1]: Stopping vsftpd FTP server...
May 22 13:13:46 my_ubuntu systemd[1]: Stopped vsftpd FTP server.
lines 1-11/11 (END)
```

Stopped HTTP server

```
ws1@ws1:~$ sudo service apache2 stop
ws1@ws1:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vend
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: inactive (dead) since Wed 2019-05-22 13:13:45 UTC; 3s ago
  Process: 1799 ExecStop=/usr/sbin/apachectl stop (code=exited, statu
  Process: 954 ExecStart=/usr/sbin/apachectl start (code=exited, stat
 Main PID: 1292 (code=exited, status=0/SUCCESS)

May 22 13:11:19 ws1 systemd[1]: Starting The Apache HTTP Server...
May 22 13:11:28 ws1 apachectl[954]: AH00558: apache2: Could not relia
May 22 13:11:28 ws1 systemd[1]: Started The Apache HTTP Server.
May 22 13:13:45 ws1 systemd[1]: Stopping The Apache HTTP Server...
May 22 13:13:45 ws1 apachectl[1799]: AH00558: apache2: Could not reli
May 22 13:13:45 ws1 systemd[1]: Stopped The Apache HTTP Server.
lines 1-15/15 (END)
```

Now we can see after stopping FTP and HTTP server nagios shows critical and is at 3 attempts.

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Users	OK	05-22-2019 17:48:11	44d 21h 34m 30s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	05-22-2019 17:44:15	1d 17h 42m 56s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0.001 second response time
	PING	OK	05-22-2019 17:44:15	22d 19h 53m 3s	1/4	PING OK - Packet loss = 0%, RTA = 0.06 ms
	RAM	OK	05-22-2019 17:44:15	0d 17h 45m 18s	1/4	OK - 2478 / 7874 MB (31%) Free Memory, Used: 2736 MB, Shared: 527 MB, Buffers + Cached: 2658 MB
	Remote Load	OK	05-22-2019 17:48:11	0d 2h 30m 3s	1/4	OK - load average: 0.94, 0.93, 0.84
proftpserver	PING	OK	05-22-2019 17:48:55	0d 0h 3m 13s	1/4	PING OK - Packet loss = 0%, RTA = 7.32 ms
	Remote Load	OK	05-22-2019 17:47:16	0d 1h 6m 6s	1/4	SNMP OK - Average:
	monitor ftp	CRITICAL	05-22-2019 17:48:50	0d 0h 2m 18s	3/4	connect to address localhost and port 21: Connection refused
students.iitmandi.ac.in	PING	OK	05-22-2019 17:48:15	0d 0h 0m 53s	1/4	PING OK - Packet loss = 0%, RTA = 93.57 ms
	Remote Load	OK	05-22-2019 17:47:52	0d 1h 6m 6s	1/4	SNMP OK - Average:
webbserver	PING	WARNING	05-22-2019 17:48:03	0d 0h 47m 54s	4/4	PING WARNING - DUPLICATES FOUND! Packet loss = 0%, RTA = 52.25 ms
	Remote Load	OK	05-22-2019 17:47:16	0d 1h 6m 6s	1/4	SNMP OK - Average:
	monitor http	CRITICAL	05-22-2019 17:48:16	0d 0h 2m 52s	3/4	connect to address localhost and port 80: Connection refused

Results 1 - 13 of 13 Matching Services

After some time

```
my_ubuntu@my_ubuntu:~$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
   Active: active (running) since Wed 2019-05-22 13:15:07 UTC; 24s ago
  Process: 2890 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, s
 Main PID: 2894 (vsftpd)
    Tasks: 1 (limit: 503)
   Memory: 588.0K
   CGroup: /system.slice/vsftpd.service
           └─2894 /usr/sbin/vsftpd /etc/vsftpd.conf

May 22 13:15:07 my_ubuntu systemd[1]: Starting vsftpd FTP server...
May 22 13:15:07 my_ubuntu systemd[1]: Started vsftpd FTP server.
lines 1-12/12 (END)
```

```
ws1@ws1:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset:
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Wed 2019-05-22 13:15:13 UTC; 2s ago
  Process: 1799 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS
  Process: 1857 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCE
 Main PID: 1873 (apache2)
    Tasks: 6 (limit: 2319)
   CGroup: /system.slice/apache2.service
           ├─1873 /usr/sbin/apache2 -k start
           ├─1878 /usr/sbin/apache2 -k start
           ├─1879 /usr/sbin/apache2 -k start
           ├─1880 /usr/sbin/apache2 -k start
           ├─1881 /usr/sbin/apache2 -k start
           └─1882 /usr/sbin/apache2 -k start

May 22 13:15:13 ws1 systemd[1]: Starting The Apache HTTP Server...
May 22 13:15:13 ws1 apachectl[1857]: AH00558: apache2: Could not reliably determ
May 22 13:15:13 ws1 systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)
```

We can see ftp and apache server being started by event-handler

Nagios interface Finally

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Users	OK	05-22-2019 17:50:11	44d 21h 36m 5s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	05-22-2019 17:49:15	1d 17h 44m 31s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0.024 second response time
	PING	OK	05-22-2019 17:49:15	22d 19h 54m 38s	1/4	PING OK - Packet loss = 0%, RTA = 0.07 ms
	RAM	OK	05-22-2019 17:49:15	0d 17h 46m 53s	1/4	OK - 2569 / 7874 MB (32%) Free Memory, Used: 2760 MB, Shared: 546 MB, Buffers + Cached: 2543 MB
	Remote Load	OK	05-22-2019 17:50:11	0d 2h 31m 38s	1/4	OK - load average: 1.10, 1.03, 0.89
proftpserver	PING	WARNING	05-22-2019 17:49:55	0d 0h 0m 48s	1/4	PING WARNING - Packet loss = 0%, RTA = 104.79 ms
	Remote Load	OK	05-22-2019 17:49:16	0d 1h 7m 41s	1/4	SNMP OK - Average:
	monitor ftp	OK	05-22-2019 17:49:50	0d 0h 0m 53s	1/4	FTP OK - 0.010 second response time on localhost port 21 [220 (vsFTPd 3.0.3)]
students.iitmandi.ac.in	PING	OK	05-22-2019 17:48:15	0d 0h 2m 28s	1/4	PING OK - Packet loss = 0%, RTA = 93.57 ms
	Remote Load	OK	05-22-2019 17:48:52	0d 1h 7m 41s	1/4	SNMP OK - Average:
webbserver	PING	WARNING	05-22-2019 17:50:03	0d 0h 49m 29s	4/4	PING WARNING - DUPLICATES FOUND! Packet loss = 0%, RTA = 174.81 ms
	Remote Load	OK	05-22-2019 17:49:16	0d 1h 7m 41s	1/4	SNMP OK - Average:
	monitor http	OK	05-22-2019 17:50:16	0d 0h 0m 27s	1/4	HTTP OK: HTTP/1.1 200 OK - 11192 bytes in 0.001 second response time

Script Screenshot

```
# What state is the NRPE service in?
case "$1" in
OK)
        # The service just came back up, so don't do anything...
        ;;
WARNING)
        # We don't really care about warning states, since the service is probably still running...
        ;;
UNKNOWN)
        # We don't know what might be causing an unknown error, so don't do anything...
        ;;
CRITICAL)
        # Aha!  The BLAH service appears to have a problem - perhaps we should restart the server...

        # Is this a "soft" or a "hard" state?
        case "$2" in

        # We're in a "soft" state, meaning that Nagios is in the middle of retrying
        SOFT)
                # What check attempt are we on?  We don't want to restart the web server on the firs\

                # check, because it may just be a fluke!
                case "$3" in

                # Wait until the check has been tried 3 times before restarting the web server.
                # If the check fails on the 4th time (after we restart the web server), the state
                # type will turn to "hard".
                # Hopefully this will restart the web server successfully, so the 4th check will
                # result in a "soft" recovery.
                3)
                        # Call NRPE to restart the service on the remote machine
                        /usr/local/nagios/libexec/check_nrpe -H 192.168.43.212 -c restart-http
                        ;;
                        esac
                ;;

        # The service somehow managed to turn into a hard error without getting fixed.
        # It should have been restarted by the code above, but for some reason it didn't.
        HARD)
                case "$3" in

                4)
                        echo -n "Restarting $6 service...\n"
                        # Call the init script to restart the NRPE server
                        /usr/local/nagios/libexec/check_nrpe -H 192.168.43.212 -c restart-http
                        ;;
                        esac
                ;;
        esac
        ;;
esac
```

10. Performance

The performance of our setup depends on how capable is it to perform good monitoring and make decisions efficiently on the basis of states of the server and perform the task of decision making. For performance check, simple nagios (without event handler – just monitoring) will be run and and the states of the servers and their services would be noted in different scenarios. Now in those scenarios, nagios with event handler would be run and again the states would be noted. The difference is the performance of our setup.

11. Limitations

It is important to note that using nagios to automatically manage servers has many restrictions which are out of hand of manager if not given proper rights.
Some of the restrictions are:

1. Nagios user needs to be provided access to remote host to be able to execute commands such as restarting a service.
2. Nagios event handler only takes effect when a state change occurs,therefore if nagios see a CRITICAL HARD state and number of attempts have exceeded maximum then for event-handler to work a state change must occcurs.
3. It is worth noting that there is only a limited way event handler can manage a server such as restarting it, because not every error that occurs in a server could be corrected by simple commands.

12. Further Improvements

Introduce a notification system to notify person responsible for a server, about what state the server is in and if the server is automatically restarted.

Expand the scale of servers nagios is monitoring and checking how capable it is in managing several servers efficiently.

13. Test Script

event_handler_script.sh – This script is being used to make decisions on basis of states of the server as shown in above diagram.
We have made 2 different scripts, “restart-http” for restarting the http server and “restart-service” for restarting the ftp server’s service.
These scripts are called by event handlers whenever the state of that service changes, not all the time, hence reducing the work done in background.

Basically what a script is doing is :

Check state of the service
    If CRITICAL
        Check whether in soft or hard state
            If SOFT
                Check the no of attempts made
                    If 3
                        Restart the server
            Else if HARD
                Check the no of attempts made
                    If 4
                        Restart the server

14. References

[1] NAGIOS
https://support.nagios.com/forum/viewtopic.php?f=6&t=50507
http://network.iitmandi.ac.in/nagios/
[2] Event Handler
https://blog.karssen.org/2010/09/14/nagios-event-handlers-for-services-on-remote-machines/
[3] For block diagrams.
https://www.lucidchart.com/
[4] NRPE :
https://assets.nagios.com/downloads/nagioscore/docs/nrpe/NRPE.pdf
[5] SMTP-
https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-on-ubuntu-18-04
[7] FTP
https://www.tecmint.com/install-ftp-server-in-ubuntu/