Network Monitoring

- Monitoring the entire infrastructue
- Detecting of any network or server problems
- Finding the cause of any issues
- Maintaining security and availiability of service
- Monitoring performances or troubleshoot
- Responding automatically to any issues

Monitoring with Nagios

Nagios®

1. Installation

- Goto: https://www.nagios.com/downloads/nagios-xi/
- Choose your platform and install Nagios
- Install from sources (Recommended!)

Nagios core
https://www.nagios.org/downloads/nagios-core/thanks/?skip=1&product_download=nagioscore-source

Plugins
https://www.nagios.org/downloads/nagios-plugins/

Follow instructions for:

- Ubuntu:
  https://www.geeksforgeeks.org/how-to-install-nagios-on-ubuntu/

- Debian:
  https://computingforgeeks.com/install-and-configure-nagios-on-debian/

2. Configuration files

- **nagios.cfg** The main configuration file of Nagios core. Contains the location of log file of Nagios, hosts and services state update interval, users and groupds, paths, etc.
- **cgi.cfg** data they might need. It contains all the user and group information and their rights and permissions.
- **resource.cfg** You can define $USERx$ macros which are useful for storing sensitive information such as usernames, passwords, etc.
- **commands.cfg** Provides command definitions. These commands are used to check and monitor hosts and services.
- **contacts.cfg** Contains contacts and groups information of Nagios. By default, one contact is already present Nagios admin.
- **templates.cfg** Provides some example object definition templates that are referred by other host, service, contact, etc.
- **timeperiods.cfg** Provides some example timeperiod definitions that you can refer in host, service, contact, and dependency definitions.

3. Continuous Monitoring

Continuous Monitoring is all about the ability of an organization to detect, report, respond, contain and mitigate the attacks that occur, in its infrastructure.

- It detects all the server and network problems.
- It finds the root cause of the failure.
- It helps in reducing the maintenance cost.
- It helps in troubleshooting the performance issues.
- It helps in updating infrastructure before it gets outdated.
- It can fix problems automatically when detected.
- It makes sure the servers, services, applications, network is always up and running.
- It monitors complete infrastructure every second.

4. Hosts and Services

Nagios is the most popular tool which is used to monitor hosts and services running in your IT infrastructure.

- Host is just like a computer; it can be a physical device or virtual.
- Services are those which are used by Nagios to check something about a host.

sudo nano /usr/local/nagios/etc/servers/ubuntu_host.cfg

```
define host {
    use linux-server
    host_name ubuntu_host
    alias Ubuntu Host
    address 192.168.1.10
    register 1
}
```

Route flapping

Route flapping is a networking issue where the state of a router constantly fluctuates within a short period of time.

For instance, if a router updates route A to be the best route in its first broadcast, then immediately withdraws it and updates route B to be the best route in its second broadcast, and again updates route A as the best route, the router is flapping.

Common causes

- **Dynamic routing:** When networks deploy dynamic routing, the routers are prone to intensive adaptive route changes. They dynamically advertise and withdraw routes based on how the network topology evolves. This results in a higher chance of route flapping.

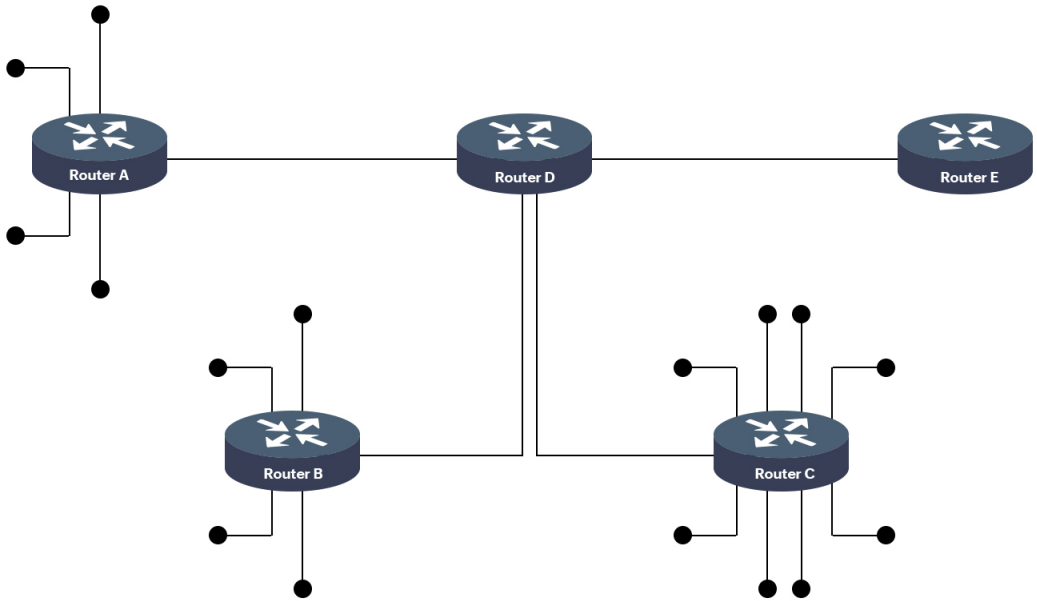
- **Misconfigurations:** Any misconfiguration, such as enabling load balancing between paths with equal hops, can easily cause route flaps.
- **Deployed protocols:** Be careful to choose between: monitor the deployment of link state and distance vector routing protocols. Since these protocols cause frequent recalculations and updates, route flapping in this scenario can hinder network convergence.
- **Hardware errors:** Faulty router hardware can cause the router state to fluctuate between up or down intensively, causing route flapping.
- **Connected devices:** Route flapping can also be due to devices associated with the router, such as a connected interface with an error or another connected router that is flapping.

Solutions to router flapping

Regularly upgrading your routers help you avoid most router issues.

Route summarization/aggregation

- Let us assume five routers (see figure in next page)
- Router D will usually have to advertise 16 routes to router E.
- However, after **route aggregation**, routers A, B, and C will each advertise only one link to router D by aggregating their links based on the common prefix.
- Router D will then aggregate these three links based on their common prefix and advertise only one route to router E.
- This greatly improves efficiency and router performance.


Router A
Router D
Router E
Router B
Router C

Route dampening

- Define a **suppress limit**. This is the preferred number of times a router is allowed to flap.
- Misconfigured route dampening metrics can easily cause parts of the network to be unreachable or even cause other routers to flap.
- Keep a close watch on your network routers.

Extra practical info

Debian live with persistence.

First try with official image from www.debian.org/CD/live/ From SE site (standard live):

wget -c https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/debian-live-11.6.0-amd64-xfce.iso

Then checksum you download file with

https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/SHA256SUMS

Ok ISO filesystem is read-only, but there is a little workaround: we could replace non vital bootparam by persistence in this way.

Once file validated ! you could alter them by using sed for replacing strings in binary.

LANG=C sed ’s/splash quiet/persistence /;s/quiet splash/persistence /’ <./debian-l

This will create a modified copy of your live binary file, by strictly replacing splash quiet or quiet splash by persistence, everywhere. Ok this will work only while grub boot command do contain this two words together.

But care to not miss the space after persistence:

"splash quiet" -> 12 characters
"persistence " -> 12 characters

Or your binary will be broken.

Install on USB key

dd if=debian-live-11.6.0-amd64-xfce-persist.iso of=/dev/sdX

Then add your third partition for persistence:

```
fdisk /dev/sdX
n               # new partition
p               # primary
<Return>        # default: 3
<Return>        # default: next free sector
<Return>        # default: last addressable sector
w               # write and quit
```

This could be run without interaction:

fdisk /dev/sdX <<<$'n\np\n\n\n\nw'

Format and prepare persistence with union:

```
mkfs.ext4 -L persistence /dev/sdX3
mount /dev/sdX3 /mnt
echo '/ union' >/mnt/persistence.conf
sync
umount /mnt
```

Then eject and try!

If you use official, unmodified image, for using persistence, you have to interrupt boot selection: Once menu screen is displayed, choose your boot option, then instead of Return, hit Tab. The kernel commandline will be displayed, then add persistence with a space, after last word (quiet), then hit Return. Unfortunately, as 1st partition is bundled with UEFI and is ISO, you can't modify the boot command.

Serial communication with Linux

- Very useful in data centers!
- Use an RS-232 serial and DB-9 serial cables.

- Find the serial port:
  $ dmesg |grep tty
- Very useful in data centers!

- Use an RS-232 serial and DB-9 serial cables.

- Find the serial port:
  $ dmesg |grep tty
  $ setserial -g /dev/ttyUSB[0123]
  $ ls /dev/serial/by-id/
- Connect the serial cable to the serial port
- Login with tio or minicom
  $ l -g /dev/ttyUSB[0123]
  $ ls /dev/serial/by-id/

- Connect the serial cable to the serial port
- Login with tio or minicom

```
$ tio /dev/ttyUSB0
```

Prefix, Network, Subnet and Host addresses

```
IP: 128.42.5.4          10000000 00101010 00000101 00000100
Subnet: 255.255.248.0   11111111 11111111 11111000 00000000
```

Prefix

```
255.255.248.0           11111111 11111111 11111000 00000000
I counted twenty-one 1s
-> /21
```

Network address

```
128.42.5.4              10000000 00101010 00000101 00000100
255.255.248.0           11111111 11111111 11111000 00000000
[Logical AND]
                        10000000 00101010 00000000 00000000

-> 128.42.0.0
```

Broadcast address

```
128.42.5.4              10000000 00101010 00000101 00000100
Host bit mask           00000000 00000000 00000hhh hhhhhhhh
[host bits]
                        10000000 00101010 00000111 11111111

-> 128.42.7.255
```

Training Exercises

Work with the Pratical Exercises in Chapter 7 of NCP_Core_Prep_Guide.pdf from Nagios. You can find a copy in my Github repository.

Challenge no 3

Continuous Monitoring with Nagios

Q1. Install and configure Nagios.

Q2. What is Nagios?

Q3. How does Nagios works?

Q4. Explain Main configuration file and its location.

Q5. What are plugins in Nagios?

Q6. Describe the difference between active and passive check.

Q7. Explain Nagios state types.

Q8. What is Flapping in Nagios?

Q9. What is State Stalking in Nagios?