P4 - GIXPD

Objectiu

Analitzar diferents eines per a la monitorització de xarxes.

Accions

1) Sobre la infraestructura de la Pràctica 1 instal·lar Nagios4 sobre la MVA y monitoritzar tant la MVA com B i C. Sobre B i C solament monitoritzar serveis externs (ping, ssh, http). Crear en B i C un arxiu (fake) fins que ocupin el 90% del disc i veure com es reflecteix això en el panel de control de Nagios.

Nota: Per crear per exemple un arxiu de 60M (fake) podeu fer servir:

truncate --size 60M sample.txt

shred --iterations 1 sample.txt

2) Realitzar una prova de monitorització amb Netdata (fer un compte en https://www.netdata.cloud/) i provar dues formes de treballar:

a) independent (standalone): Instal·lant netdata del repositori Debian sobre A.
b) a través de https://app.netdata.cloud instal·lar i monitoritzar B i C (recordar de fer servir el codi wget... que us instal·larà el programari però connectat al cloud de Netdata).

NB: Si es desitja posar A sobre app.netdata.cloud s'haurà de desinstal·lar totalment apt remove –purge ...) la versió standalone verificant que no quedi cap paquet de netdata i tornar a instal·lar-ho amb el codi wget ... (com s'ha fet en B i C).

Tools?

Es important mesurar el rendiment de la xarxa i per això es necessiten eines.

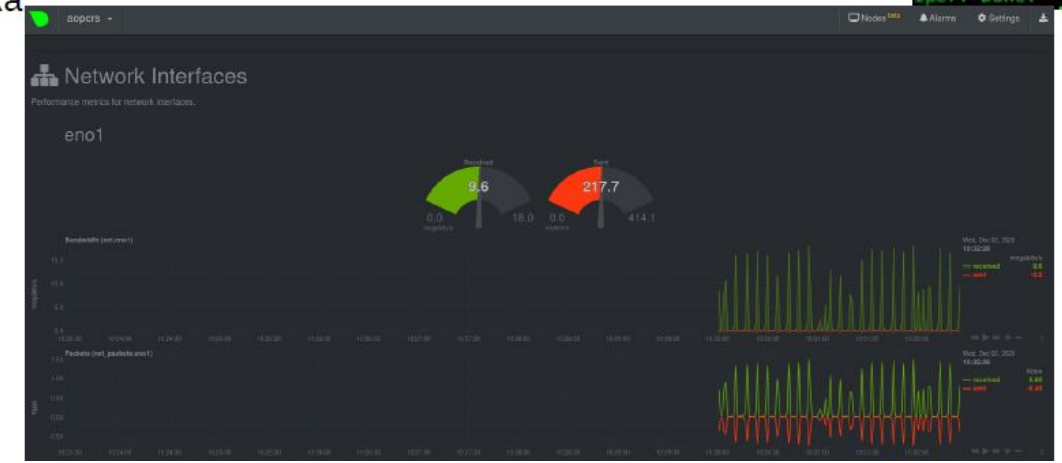
Iperf: eina simple que permet mesurar el rendiment de la xarxa. Requereix un client i un servidor (dos dispositius un funcionant com a servidor i l'altre com a client que fa sol·licituds al servidor). iperf3 -s per executar-lo en mode servidor. El port de servidor per defecte és 5201: **apt install iperf3**

iperf -s (al servidor) iperf3 -c IP_SERVER (al client)

```
root@mybi:~# iperf3 -c 20.20.21.14
Connecting to host 20.20.21.14, port 5201
[  4] local 20.20.21.20 port 48480 connected to 20.20.21.14 port 5201
[ ID] Interval           Transfer     Bandwidth       Retr  Cwnd
[  4]   0.00-1.01   sec  92.2 MBytes   770 Mbits/sec   96    100 KBytes
[  4]   1.01-2.00   sec   109 MBytes   920 Mbits/sec  106    195 KBytes
[  4]   2.00-3.00   sec   114 MBytes   954 Mbits/sec  207   97.6 KBytes
[  4]   3.00-4.00   sec   108 MBytes   903 Mbits/sec  108    140 KBytes
[  4]   4.00-5.00   sec   109 MBytes   918 Mbits/sec  189    163 KBytes
[  4]   5.00-6.00   sec   104 MBytes   868 Mbits/sec  283    143 KBytes
[  4]   6.00-7.00   sec   107 MBytes   893 Mbits/sec  199    236 KBytes
[  4]   7.00-8.02   sec  98.9 MBytes   816 Mbits/sec  217    168 KBytes
[  4]   8.02-9.00   sec  96.6 MBytes   825 Mbits/sec   64    187 KBytes
[  4]   9.00-10.00  sec   110 MBytes   926 Mbits/sec  305    107 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Retr
[  4]   0.00-10.00  sec  1.02 GBytes   879 Mbits/sec  1774             sender
[  4]   0.00-10.00  sec  1.02 GBytes   877 Mbits/sec                  receiver

iperf Done.
```

Netdata: Hem d'anar en compte ja que ens permet veure el rendiment de la xarxa de la nostra màquina no el rendiment de la xarxa



ping / hping3: en el cas que no tenim posibilitat per accedir al host remot.

La taxa de bits d'un sol ping ve donada per:

Mida PING * 8 bits / byte / RTT

Per tant, si s'envien 1000 ping de mida de 5.000 bytes i s'obté un RTT mitjà de 100 msec, es pot dir

5000 * 8 / 0,1 = 400.000 bps

Tools?

Ntopng: és la nova versió del ntop original, una eina de mesura de trànsit de xarxa que controla l'ús de la xarxa. ntopng es basa en libpcap/PF_RING i s'ha escrit de forma portàtil per tal d'executar-se virtualment en totes les plataformes Unix, Mac OS X i Windows. Proporciona una interfície d'usuari web encriptada i intuïtiva per explorar informació de trànsit en temps real i històrica. **apt install ntopng navegador: localhost:3000**

Online: https://www.dotcom-tools.com/website-speed-test.aspx

Netperf: **apt isntall**

netperf -H 10.142.0.93 -l 10 -t TCP_RR -v 2

ping -c 10 -i 0.01

Diferencias explicadas en:
https://cloud.google.com/blog/products/networking/using-netperf-and-ping-to-measure-network-latency

BandwidthD (2005)

Eines generals que inclouen Network com un apartat més (analitzades en monitorització)

- Cacti
- Ganglia
- Icinga
- Nagios
- Collectd
- Munin
- Zabbix

Docker:

Nagios jasonrivers/nagios (usuari i passwd: nagiosadmin / nagios).
https://github.com/JasonRivers/Docker-Nagios

Ganglia: https://github.com/kurthuwig/docker-ganglia

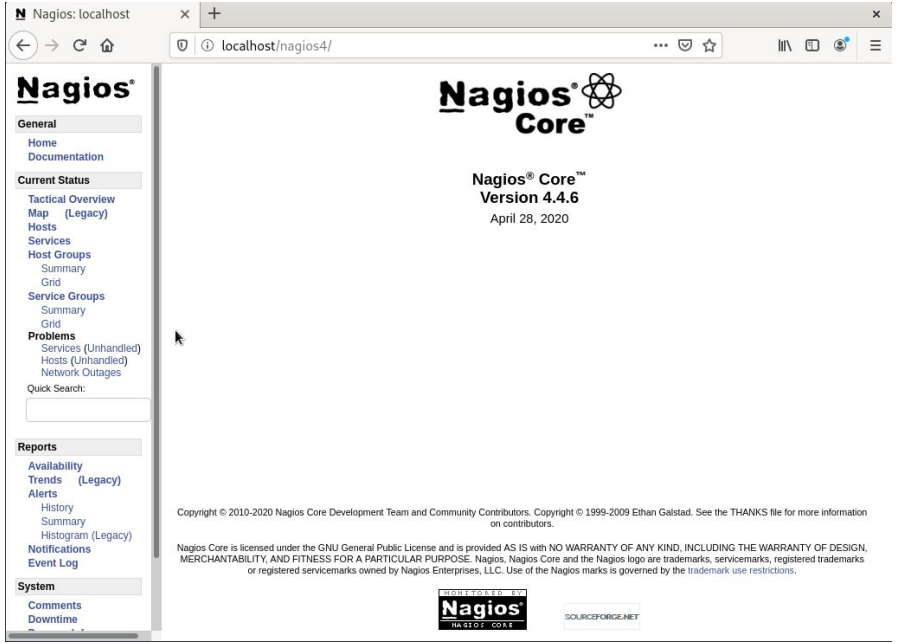
Icinga: https://github.com/utopia-planitia/icinga1-images
https://hub.docker.com/r/utopiaplanitia/icinga1-server

NAGIOS MAIN HOST

=> Configurar nombres de host y archivo hosts para los hosts
$ apt-cache policy nagios4
$ nano /etc/apt/sources.list
=> añadimos en todas la entradas de Debian: “contrib non-free”
$ apt update
$ clear
$ apt-cache policy nagios4
$ apt install nagios4
$ clear
$ apt update
$ getent passwd nagios
$ getent group nagios
$ systemctl status nagios4
$ systemctl enable nagios4
$ ls -1d /etc/nagios4/*
$ nano /etc/apache2/conf-available/nagios4-cgi.conf
=> Observar estructura
$ a2enmod rewrite cgi
$ systemctl restart apache2
$ nagios4 -v /etc/nagios4/nagios.cfg
=> Test de validación Nagios4: Total Warnings: 0 y Total Errors: 0
=> Con esto ya podemos acceder al navegador e ir a: **localhost/nagios4**
$ sudo apt install nagios-plugins nagios-nrpe-plugin => para el test posterior

$ cp /etc/nagios4/localhost.cfg /etc/nagios4/client01.cfg
$ nano /etc/nagios4/nagios.cfg => añadimos línea, debajo de la que hay del mismo tipo: cfg_file=/etc/nagios4/objects/client01.cfg (este es copia de localhost.cfg adaptado)

Evaluar los diferentes elementos del archivo copiado.
¿Qué ajustar en el contenido del archivo copiado como mínimo?



NAGIOS - CLIENT HOST

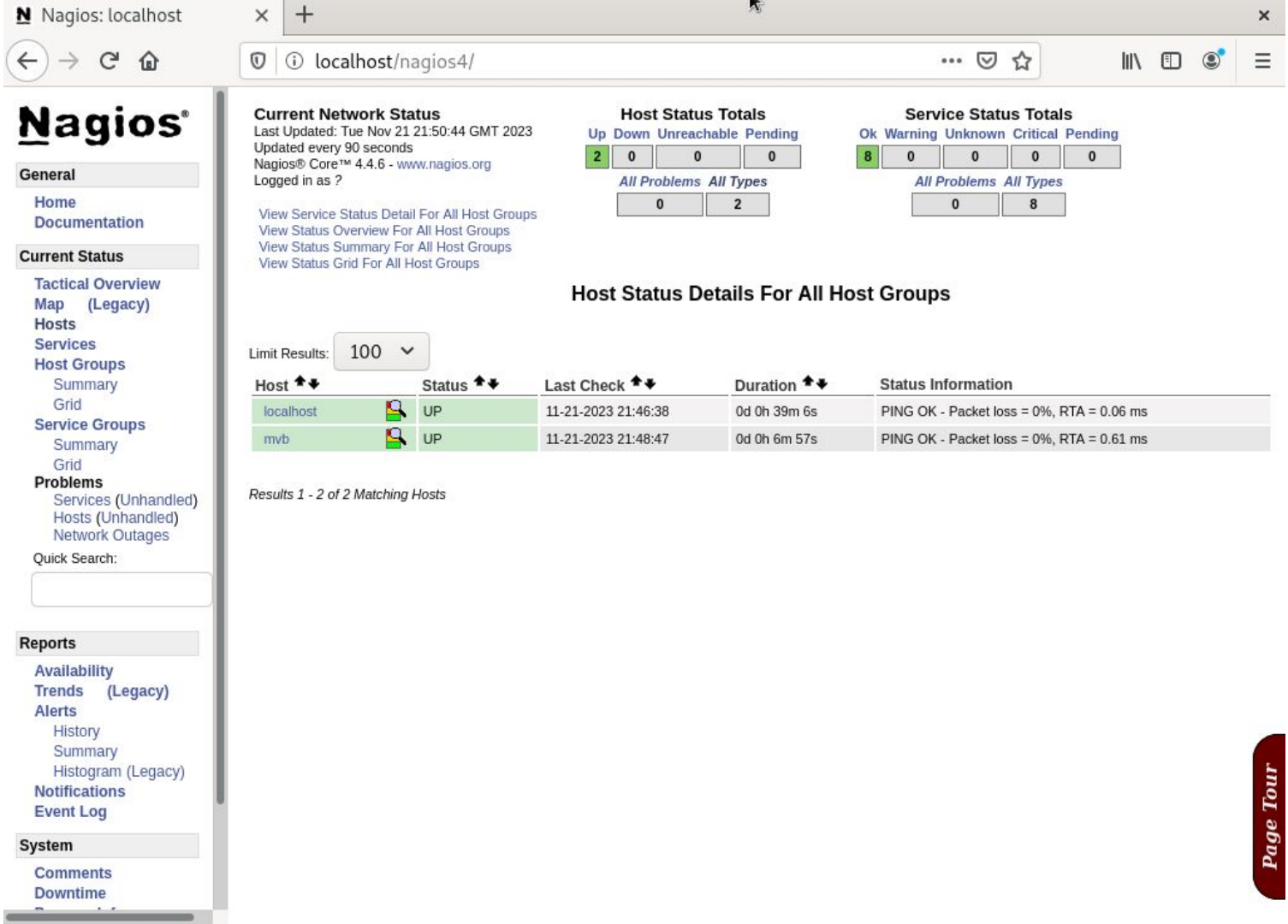
$ apt install nagios-nrpe-server nagios-plugins
$ cd /etc/nagios
$ ls -l
$ nano nrpe.cfg
⇒ server_address=20.20.21.220 (IP del cliente, la máquina en la que editamos este archivo: mvb)
=> allowed_hosts=127.0.0.1,::1,**20.20.21.219** (IP máquina servidor NAGIOS: mva)
$ systemctl restart nagios-nrpe-server.service
$ systemctl enable nagios-nrpe-server
$ systemctl status nagios-nrpe-server

$ editamos en cliente(mvb): nano /etc/nagios/nrpe.cfg y actualizamos ip de mvb en servidor y añadimos ip del servidor Nagios:
  => server_address=20.20.21.220 (ip mvb)
  => allowed_hosts=127.0.0.1,::1,20.20.21.219 (mva, servidor Nagios)
$ systemctl restart nagios-nrpe-server.service
$ systemctl enable nagios-nrpe-server
$ systemctl status nagios-nrpe-server

¿Necesario actualizar el archivo: **nrpe_local.cfg**?

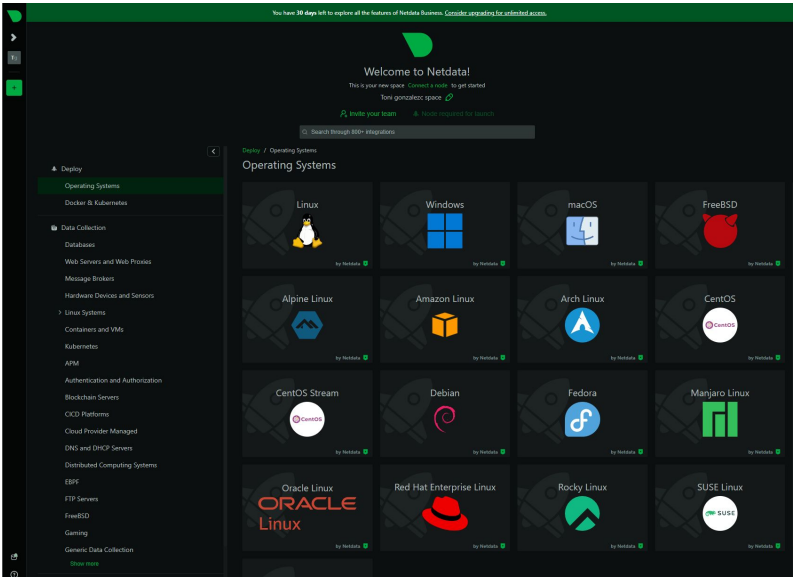
```
command[check_root]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /
command[check_ping]=/usr/lib/nagios/plugins/check_ping -H 10.5.5.12 -w 100.0,20% -c 500.0,60% -p 5
command[check_ssh]=/usr/lib/nagios/plugins/check_ssh -4 10.5.5.12
command[check_http]=/usr/lib/nagios/plugins/check_http -I 10.5.5.12
command[check_apt]=/usr/lib/nagios/plugins/check_apt
```

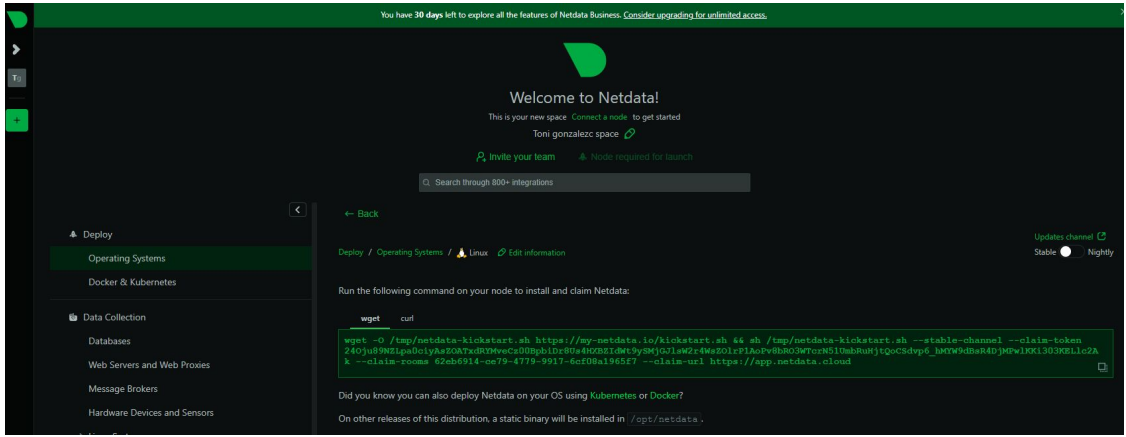
NAGIOS

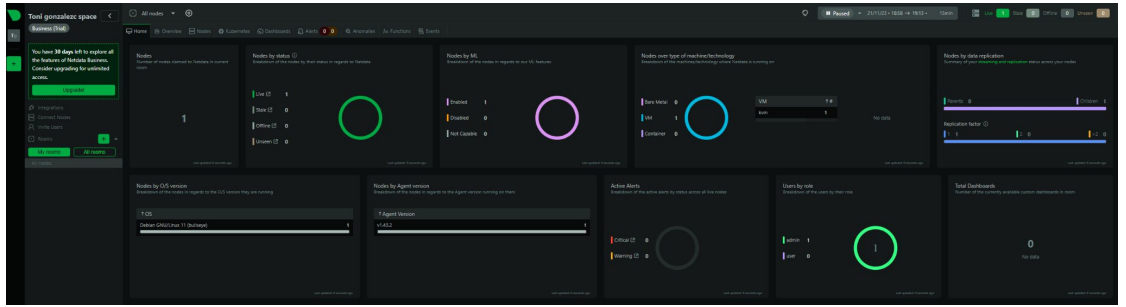

Nagios: localhost
localhost/nagios4/
Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages
Quick Search:
Reports
Availability
Trends (Legacy)
Alerts
History
Summary
Histogram (Legacy)
Notifications
Event Log
System
Comments
Downtime
Current Network Status
Last Updated: Tue Nov 21 21:50:44 GMT 2023
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as ?
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 All Types
0 2
Service Status Totals
Ok Warning Unknown Critical Pending
8 0 0 0 0
All Problems All Types
0 8
Host Status Details For All Host Groups
Limit Results: 100
Host
Status
Last Check
Duration
Status Information
localhost
UP
11-21-2023 21:46:38
0d 0h 39m 6s
PING OK - Packet loss = 0%, RTA = 0.06 ms
mvb
UP
11-21-2023 21:48:47
0d 0h 6m 57s
PING OK - Packet loss = 0%, RTA = 0.61 ms
Results 1 - 2 of 2 Matching Hosts
Page Tour

Netdata

Registrarse en https://www.netdata.cloud







Stand Alone

$ clear
$ apt update
$ apt install netdata -y
$ cd /etc/netdata/
$ ls -l
$ nano netdata.conf
$ ip a
$ nano netdata.conf => sustituir la ip local: 127.0.0.1 por la ip de la interface local seleccionada (en nuestro caso: 20.20.20.175)
$ systemctl restart netdata.service

Ahora ir al navegador a: **http://<IP Adress>:19999** (puede que tarde un rato en inciarse…)
En nuestro caso: **http://20.20.20.175:19999**

Accions

3. a) Fent servir dues MV a ON determinar el rendiment de la xarxa 20.20.20.0/23 a través de les eines que hem vist en classe que consideri més adient. Fer proves de càrrega de la xarxa (per exemple copiant un arxiu entre les màquines p.ex. amb l'ordre scp alhora que mesuren les prestacions). Extraure conclusions.

b) Fer una anàlisi de la xarxa 10.10.10.0/24 i de la 20.20.20.0/23 a través de l'eina ntopng sobre una MV de ON.

4) Extraure conclusions, avantatges i inconvenients de les eines desplegades i fer un breu anàlisi crític d'elles.

Material addicional:

Netdata: https://learn.netdata.cloud/

https://learn.netdata.cloud/docs/configuring/configuration

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

https://kifarunix.com/install-nagios-on-debian-11/?expand_article=1

Iperf3: https://iperf.fr/

https://www.goanywhere.com/blog/how-to-measure-network-and-disk-throughput-with-iperf3

Ntopng: https://www.ntop.org/products/traffic-analysis/ntop/

Ntopng

$ apt update
$ apt install software-properties-common wget
$ source /etc/os-release
$ wget https://packages.ntop.org/apt/$VERSION_CODENAME/all/apt-ntop.deb
$ apt install ./apt-ntop.deb
$ apt update && apt install ntopng
$ systemctl status ntopng.service
$ ss -tunelp | grep ntop

Navegador: 127.0.0.1:3000
Usr y pwd por defecto: admin admin
(contraseña mínimo 5 caracteres)