PRÀCTICA 4:

Monitorització de xarxes

Nom 1: David Morillo Massagué
NIU 1: 1666540
Nom 2: Adrià Muro Gómez
NIU 2: 1665191

Usuari utilitzat a la pràctica: gixpd-ged-22

Taula de continguts

Introducció

En aquesta pràctica hem explorat diverses eines i metodologies per analitzar i monitoritzar el rendiment de la xarxa i els serveis associats. Aquesta pràctica es basa en una infraestructura creada anteriorment, i inclou la instal·lació, configuració i utilització d'eines com Nagios4, Netdata, iperf3, iotop i iftop. També hem realitzat proves de càrrega i anàlisi de prestacions en diferents segments de xarxa, així com monitorització de serveis crítics.

L'objectiu principal és adquirir coneixements pràctics en la configuració i ús d'aquestes eines per a entorns reals, enfocant-nos en la seva utilitat, avantatges i limitacions.

Objectius

L'objectiu general de la pràctica és analitzar diferents eines per a la monitorització de xarxes i aplicar-les en un entorn simulat. Els objectius específics són els següents:

1. Instal·lar i configurar Nagios4:
    - Monitoritzar serveis crítics (ping, SSH, HTTP) sobre màquines virtuals específiques (MVA, B i C).
    - Simular un escenari d'alt ús del disc (90%) i analitzar com Nagios reflecteix aquesta situació en el panell de control.
2. Provar la monitorització amb Netdata:
    - Treballar en mode independent (standalone) instal·lant Netdata sobre la MVA.
    - Monitoritzar les màquines B i C a través de la plataforma Netdata Cloud per explorar les funcionalitats remotes.
3. Avaluar el rendiment de la xarxa:
    - Utilitzar eines de mesura (iperf3, scp, etc.) per analitzar el rendiment de la xarxa 20.20.20.0/23.
    - Provar càrregues simultànies i extreure conclusions sobre les prestacions.

Procediment i Desenvolupament

Monitorització amb Nagios4

En primer lloc, es va assegurar que el sistema estigués completament actualitzat. Es va utilitzar la comanda *apt update* per actualitzar la llista de paquets disponibles i, tot seguit, *apt full-upgrade* per instal·lar les versions més recents dels paquets al sistema.

Posteriorment, es van instal·lar totes les dependències necessàries per al funcionament de Nagios. Això es va fer utilitzant *apt install* per instal·lar paquets com ara *vim, wget, curl, apache2*, i altres llibreries essencials com *openssl i libssl-dev.* Aquestes eines són fonamentals per garantir la funcionalitat completa de Nagios i la seva interfície web.

```
sudo apt install vim wget curl build-essential unzip openssl libssl-dev apache2 php libapache2-mod-php php-gd libgd-dev
```

Es va descarregar la versió més recent de Nagios Core des del repositori oficial de GitHub. Es va utilitzar *wget* per obtenir l'arxiu comprimit del codi font i, després, tar per extreure el seu contingut en un directori temporal. Això va preparar els fitxers per a la compilació i instal·lació.

```
wget -O nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.4.14.tar.gz
```

A continuació, es va procedir a compilar el codi font de Nagios. Amb la comanda *./configure* --with-httpd-conf=/etc/apache2/sites-enabled, es va especificar que els fitxers de configuració d'Apache estarien disponibles en aquest directori. Això va preparar Nagios per integrar-se correctament amb el servidor web.

Es van instal·lar els fitxers que converteixen Nagios en un servei del sistema. Amb *make install-daemoninit*, es van configurar els scripts d'inici per assegurar que Nagios s'executa automàticament quan el sistema arrenca.

A més, es va configurar Apache per servir la interfície web de Nagios. Es va utilitzar *make install-webconf* per instal·lar els fitxers de configuració i *a2enmod rewrite cgi* per activar els mòduls CGI i de reescriptura.

Un pas important va ser configurar l'autenticació web. Amb la comanda *htpasswd -c /usr/local/nagios/etc/htpasswd.users blazikenadmin*, es va crear un usuari "*blazikenadmin*" per accedir a la interfície web, assignant-li una contrasenya segura.

Els plugins oficials de Nagios es van descarregar, compilar i instal·lar. Es va utilitzar *wget* per obtenir l'arxiu comprimit dels plugins, tar per extreure'ls i ./configure per preparar-los per la instal·lació.

```
root@ma:/usr/local/nagios/libexec# ls
check_apt        check_icmp           check_ntp        check_ssh
check_breeze     check_ide_smart      check_ntp_peer   check_ssl_validity
check_by_ssh     check_ifoperstatus   check_ntp_time   check_ssmtp
check_clamd      check_ifstatus       check_nwstat     check_swap
check_cluster    check_imap           check_oracle     check_tcp
check_dhcp       check_ircd           check_overcr     check_time
check_dig        check_jabber         check_ping       check_udp
check_disk       check_load           check_pop        check_ups
check_disk_smb   check_log            check_procs      check_uptime
check_dns        check_mailq          check_real       check_users
check_dummy      check_mrtg           check_rpc        check_wave
check_file_age   check_mrtgtraf       check_sensors    negate
check_flexlm     check_nagios         check_simap      remove_perfdata
check_ftp        check_nntp           check_smtp       urlize
check_hpjd       check_nntps          check_snmp       utils.pm
check_http       check_nt             check_spop       utils.sh
```

Com es pot observar a la captura de pantalla els plugins han estat instal·lats correctament.

Una vegada s'instala nagios, automàticament es defineix el host local (mva) així com els serveis que es monitoritzen sobre aquest. Per definir els hosts B i C es va crear un nou fitxer (b_c_hosts.cfg) que inclou, per cada host, el seu nom, àlies i adreça IP.

```
define host {
    use             linux-server
    host_name       MVB
    alias           MB
    address         20.20.20.72   # IP de MVB
}

define host {
    use             linux-server
    host_name       MVC
    alias           MC
    address         20.20.20.124  # IP de MVC
}
```

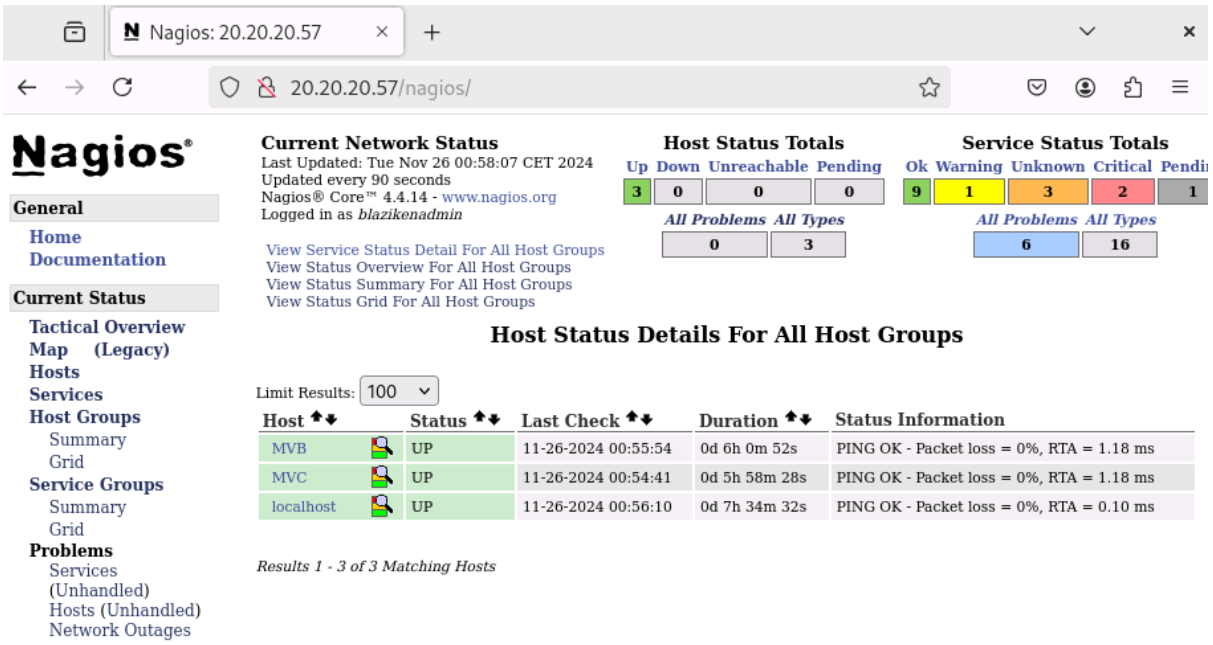
Per especificar els serveis monitoritzats (ping, ssh i http) es van configurar utilitzant els plugins instal·lats. Això assegura que Nagios pot verificar l'estat dels serveis externs de manera remota. Els serveis s'inclouen en el mateix document dels hosts (b_c_hosts).

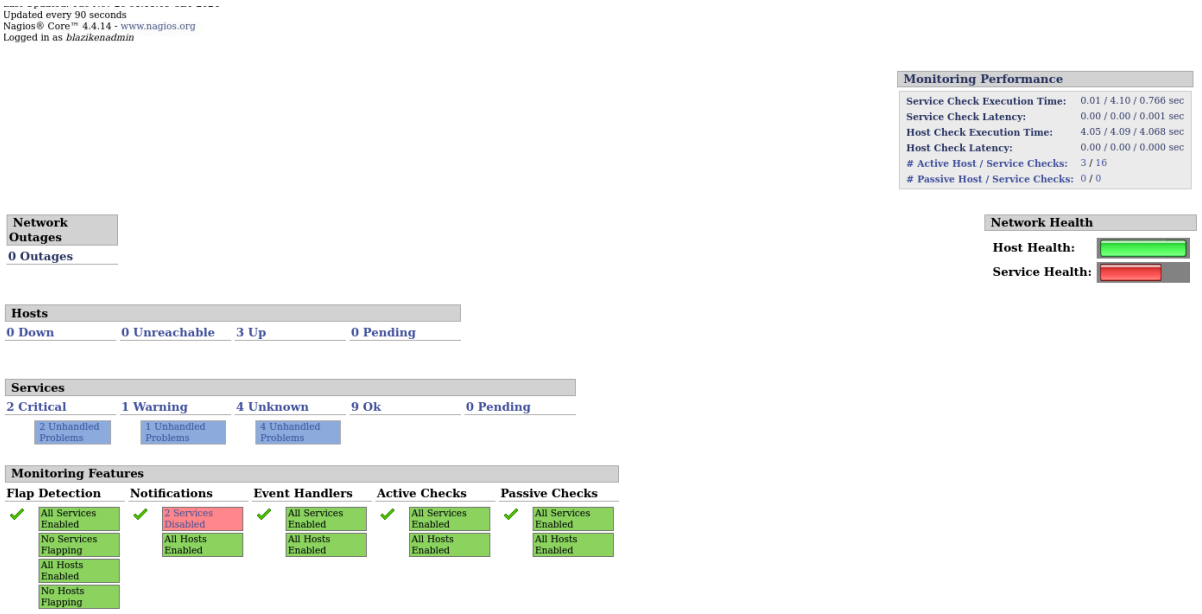
```
define service {
    use                     generic-service
    host_name               MVB
    service_description     PING
    check_command           check_ping!100.0,20%!500.0,60%
}

define service {
    use                     generic-service
    host_name               MVB
    service_description     SSH
    check_command           check_ssh
}

define service {
    use                     generic-service
    host_name               MVB
    service_description     HTTP
    check_command           check_http
}

define service {
    use                     generic-service
    host_name               MVC
    service_description     PING
    check_command           check_ping!100.0,20%!500.0,60%
}

define service {
    use                     generic-service
    host_name               MVC
    service_description     SSH
    check_command           check_ssh
}

define service {
    use                     generic-service
    host_name               MVC
    service_description     HTTP
    check_command           check_http
}
```

També es va afegir com a servei monitoritzat el check_local_disk per veure com es veu reflectit l'ús del disc en el panell de control de nagios.

```
define service {
    use                     generic-service
    host_name               MVB
    service_description     Disk Usage
    check_command           check_local_disk!20%!10%
}

define service {
    use                     generic-service
    host_name               MVC
    service_description     Disk Usage
    check_command           check_local_disk!20%!10%
}
```

Finalment, es va accedir a la interfície web de Nagios mitjançant un navegador. Introduint l'adreça IP de la MVA (20.20.20.57) seguida de "/nagios", es va obrir la pàgina d'inici de sessió, on es van utilitzar les credencials "blazikenadmin" creades anteriorment. Un cop autenticat, es van verificar els estats dels serveis configurats.





Observem que nagios ha reconegut els tres hosts (MVA, MVB, MVC) mostrant-los actius a la interfície web. No obstant, durant el transcurs de la pràctica, hi havia serveis que mostraven error i al cap d'uns minuts resultaven en operatius. Considerem que l'objectiu d'utilitzar nagios s'ha complert i considerem els errors aquests fallades del sistema per la poca capacitat de les màquines virtuals i de la xarxa.

Un dels requisits de la pràctica era simular un escenari en què els discos dels hosts B o C arribessin al 90% de la seva capacitat i observar com aquest fet es reflectia al panell de control de Nagios.

Per assolir aquest objectiu, es va crear un fitxer gran al host B, fins a ocupar el 90% del seu espai disponible. Això es va fer mitjançant la generació d'un fitxer "fake" utilitzant comandes com *truncate --size 60M sample.txt* i *shred --iterations 1 sample.txt* que permeten crear arxius de mida específica.

Un cop el disc va arribar a la capacitat desitjada, es va verificar l'estat dels sistemes utilitzant la comanda df -h, comprovant que el host B reportava un ús proper al 90% en les seves particions principals. La següent captura mostra l'ús de disc reportat per aquest host on s'observa que el disc principal /dev/vda1 està al 90% utilitzat:

```
Filesystem            Size  Used Avail Use% Mounted on
udev                  1.9G     0  1.9G   0% /dev
tmpfs                 392M  856K  391M   1% /run
/dev/vda1              16G   14G  1.6G  90% /
tmpfs                 2.0G     0  2.0G   0% /dev/shm
tmpfs                 5.0M     0  5.0M   0% /run/lock
/dev/vda15            124M   12M  113M  10% /boot/efi
20.20.20.57:/nfs_tmp   16G  4.2G   11G  28% /nfs_client
tmpfs                 392M   56K  392M   1% /run/user/1000
/dev/sr0              364K  364K     0 100% /media/adminp/CONTEXT
```

En el panell de Nagios, gràcies al servei check_local_disk configurat anteriorment, es van poder monitoritzar els estats dels discos dels hosts B i C. Les alertes reflectien la situació següent:

Host B: Estat Critical per haver superat el llindar crític del 90%.

MVB	Disk Usage	CRITICAL	11-26-2024 00:59:54	0d 0h 5m 38s	3/3	CRITICAL - USAGE OVER 90%
	HTTP	WARNING	11-26-2024 00:59:32	0d 6h 4m 22s	3/3	HTTP WARNING: HTTP/1.1 400 Bad Request - 486 bytes in 0.004 second response time
	PING	OK	11-26-2024 00:57:18	0d 6h 5m 14s	1/3	PING OK - Packet loss = 0%, RTA = 1.16 ms

Host C: Estat OK, ja que no s'havia saturat el disc.

MVC	Disk Usage	OK	11-26-2024 01:04:07	0d 0h 4m 28s	3/3	OK - enough space 23% usage
	HTTP	CRITICAL	11-26-2024 01:01:31	0d 7h 9m 31s	3/3	connect to address 20.20.20.124 and port 80: Connection refused
	PING	OK	11-26-2024 01:05:40	0d 6h 6m 45s	1/3	PING OK - Packet loss = 0%, RTA = 1.07 ms
	SSH	UNKNOWN	11-26-2024 01:02:56	0d 7h 13m 36s	3/3	Usage:

Aquest experiment demostra com Nagios és capaç de detectar i alertar automàticament sobre l'ús excessiu de recursos crítics com l'espai en disc, ajudant així a prevenir problemes futurs en els sistemes monitoritzats.

Monitorització amb Netdata

Per complementar la monitorització realitzada amb Nagios, s'ha dut a terme una prova amb Netdata, una eina especialitzada en la visualització en temps real de mètriques del sistema. Aquesta prova s'ha plantejat en dues modalitats:

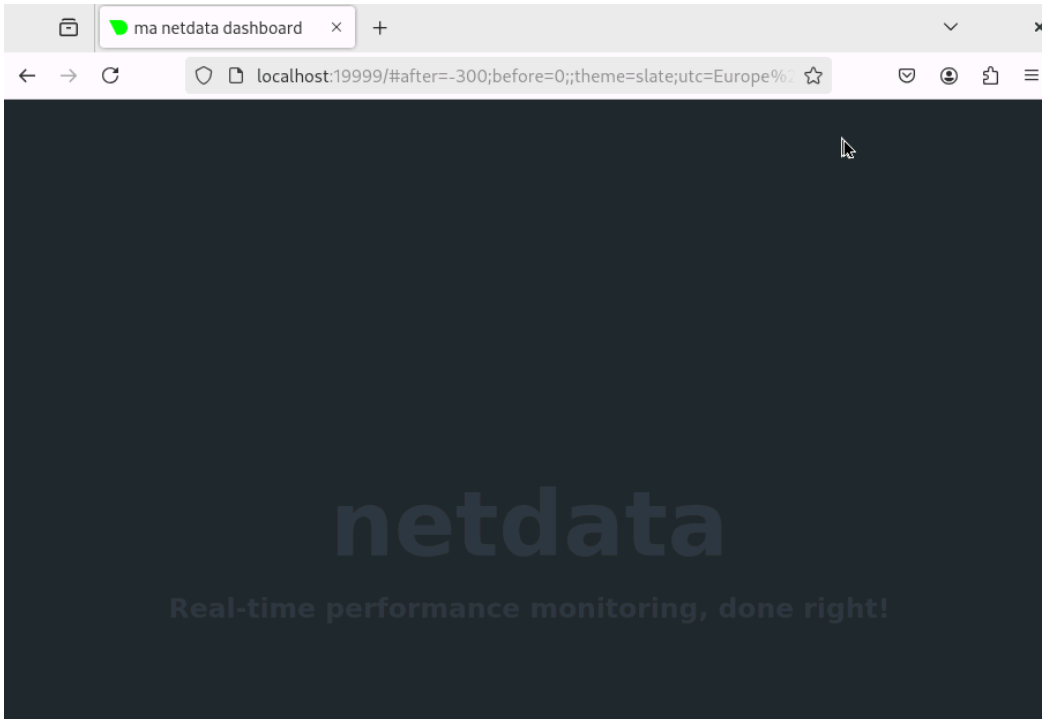
Modalitat Independent (Standalone)

En aquesta configuració, es va instal·lar Netdata directament a la MVA (A) des del repositori oficial de Debian. El procés va consistir en:

Actualitzar el sistema i instal·lar Netdata utilitzant els paquets del repositori oficial de Debian.

```
root@ma:~# apt install netdata
```

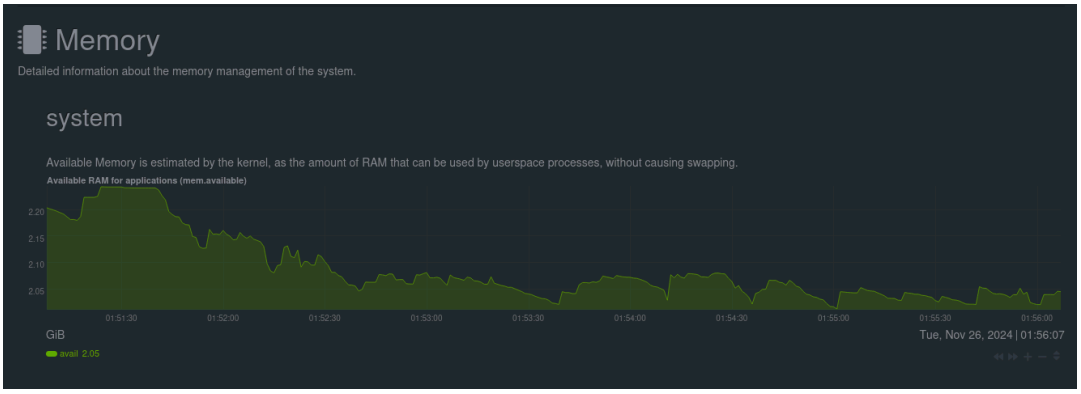
Verificar que Netdata estava actiu i accessible localment a través del navegador, utilitzant l'adreça *http://localhost:19999*.



Des d'aquesta instal·lació, es va obtenir una visió detallada de les mètriques de sistema de la MVA, incloent:

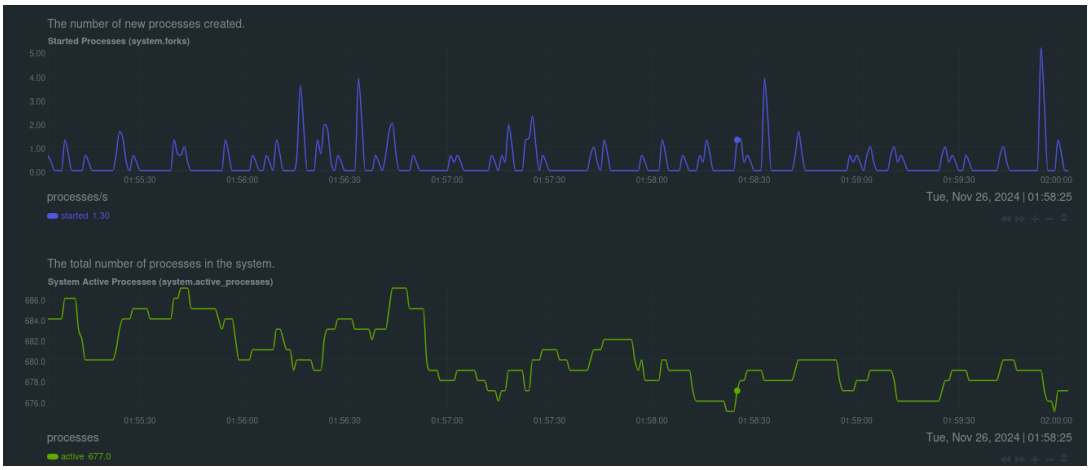
- CPU

- Memòria



- Trànsit de xarxa

- Altres paràmetres



Aquesta configuració no estava connectada al servei al núvol de Netdata, per la qual cosa la monitorització només estava disponible localment.

Monitorització amb app.netdata.cloud

La segona part de la prova va consistir a instal·lar Netdata als hosts B i C, connectant-los al servei al núvol de Netdata per centralitzar la monitorització.

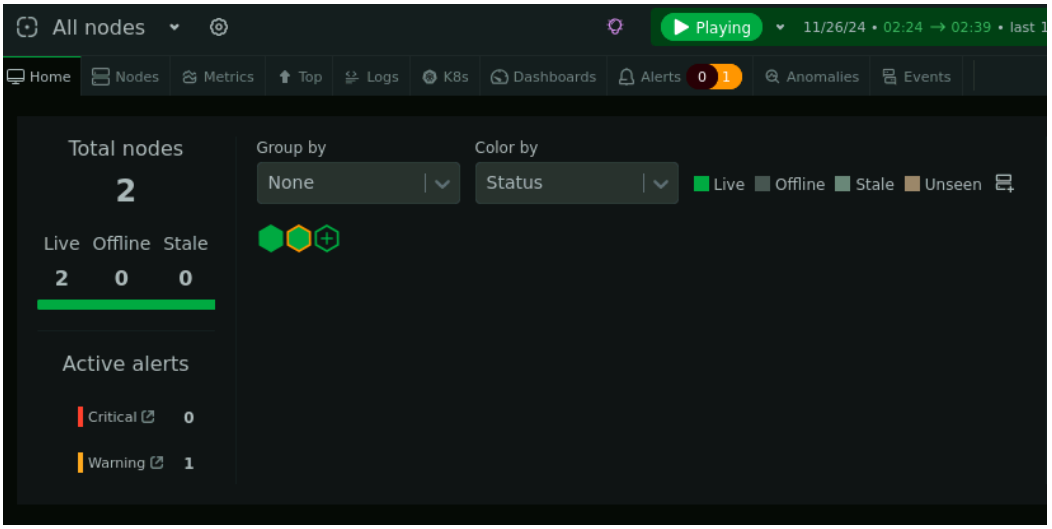
Primer, es va accedir a la pàgina oficial de Netdata Cloud (https://app.netdata.cloud/) i es va registrar un compte d'usuari. Un cop registrat, es va procedir a afegir les màquines que es desitjava monitoritzar.

Des de la interfície de Netdata Cloud, es va obtenir un codi *wget* específic per cada màquina, que incloïa un token únic associat al compte. Aquest codi permet la instal·lació del programari Netdata i la connexió automàtica a la plataforma al núvol.

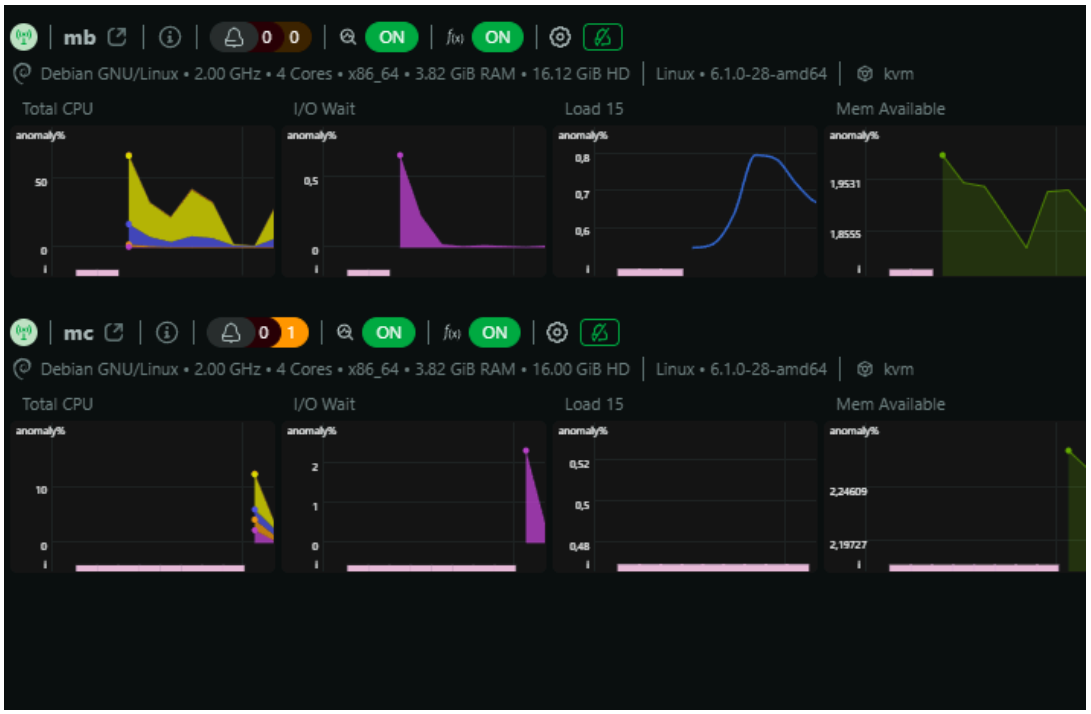
```
root@mb:~# wget -O /tmp/netdata-kickstart.sh https://get.netdata.cloud/kickstart
.sh && sh /tmp/netdata-kickstart.sh --stable-channel --claim-token OP-HFh9Dc7PeI
P3T1BcZG2Nl1Im6Mv2vTQpVB-xCmLzPRSEbT1-dGbwOBZToKPelEblN6FIDyjfA9AQu6_B_apxwyJdN
82CRujrwM56npWXDmMhulQDbRvAWoDf6Rjm8PI8h7c --claim-rooms 9e611bdb-d492-4ef0-bb0
-fc8b9566ab40 --claim-url https://app.netdata.cloud
--2024-11-26 02:29:26--  https://get.netdata.cloud/kickstart.sh
Resolving get.netdata.cloud (get.netdata.cloud)... 172.67.36.172, 104.22.78.229,
 104.22.79.229, ...
Connecting to get.netdata.cloud (get.netdata.cloud)|172.67.36.172|:443... conne
ted.
HTTP request sent, awaiting response... 200 OK
Length: 93645 (91K) [application/octet-stream]
Saving to: '/tmp/netdata-kickstart.sh'

/tmp/netdata-kickst 100%[===================>]  91.45K  --.-KB/s    in 0.02s

2024-11-26 02:29:26 (5.28 MB/s) - '/tmp/netdata-kickstart.sh' saved [93645/9364
]
```

Cada màquina (en aquest cas B i C) va executar la comanda proporcionada des de la consola. Això va instal·lar Netdata, va configurar-lo automàticament i va establir la connexió amb el compte de Netdata Cloud.

Després de completar aquest procés, es va comprovar a la interfície de Netdata Cloud que les màquines B i C apareixien com a monitoritzades.



En el panell es mostraven mètriques detallades en temps real, com ara ús de CPU, memòria, estat del disc i tràfic de xarxa.



En aquest procés, hem configurat amb èxit la monitorització de les màquines B i C mitjançant Netdata Cloud, un sistema que permet visualitzar en temps real els recursos dels servidors. Un cop registrats els servidors al núvol de Netdata, es poden visualitzar totes les mètriques rellevants, millorant així la gestió i supervisió de les màquines de manera remota i eficient.

Anàlisis de rendiment de Xarxa

En aquest apartat, l'objectiu és el d'analitzar el rendiment de la xarxa a 20.20.20.0/23 específicament, amb eines vistes a classe. Per a aquestes proves s'utilitzaran les màquines de la primera pràctica: MA, MB i MC. Recordem que MA té dues interfícies, una per la xarxa externa 10.10.10.0/24 i una per la interna 20.20.20.0/23. MB i MC estàn conectades a la xarxa interna 20.20.20.0/23 solament.

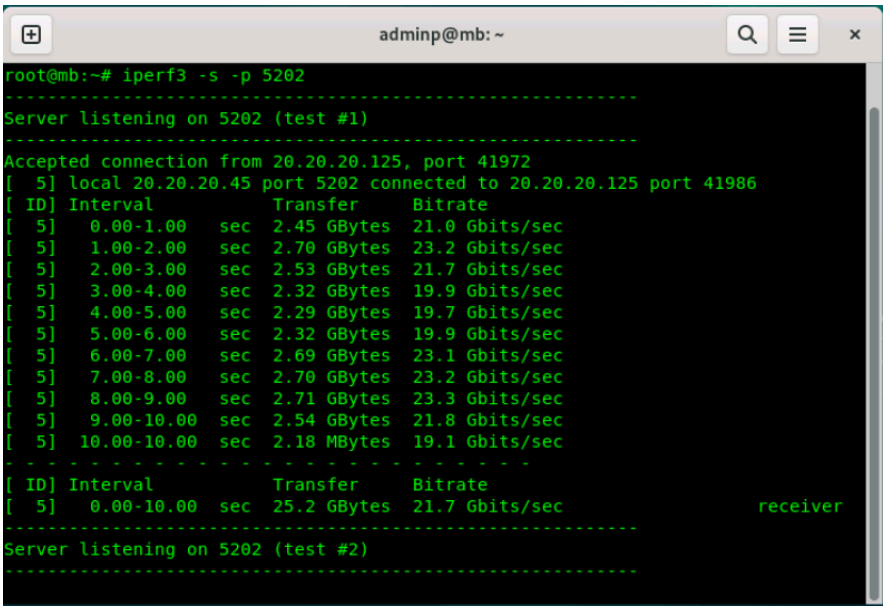
La primera de les eines és iPerf3, que permet mesurar l'amplada de banda, latència i pèrdues de paquets, mitjançant proves client-servidor, en una xarxa:

Anàlisi amb iPerf3

Per a aquesta prova, utilitzarem les màquines MB i MC, ja que només estan directament connectades a la xarxa interna (per evitar interferències amb altres xarxes o connexions involuntàries a xarxes externes)

Després d'obtenir la aplicació fent servir *sudo apt install iperf3*, executem a la comanda *iperf3 -s -p 5202* en l'ordinador servidor MVB amb els següents paràmetres:

- paràmetre **-s** per a que actuï com a servidor de la prova d'iperf3
- paràmetre **-p** per a fer servir el port 5202, ja que el predeterminat (5201) ja estava en ús

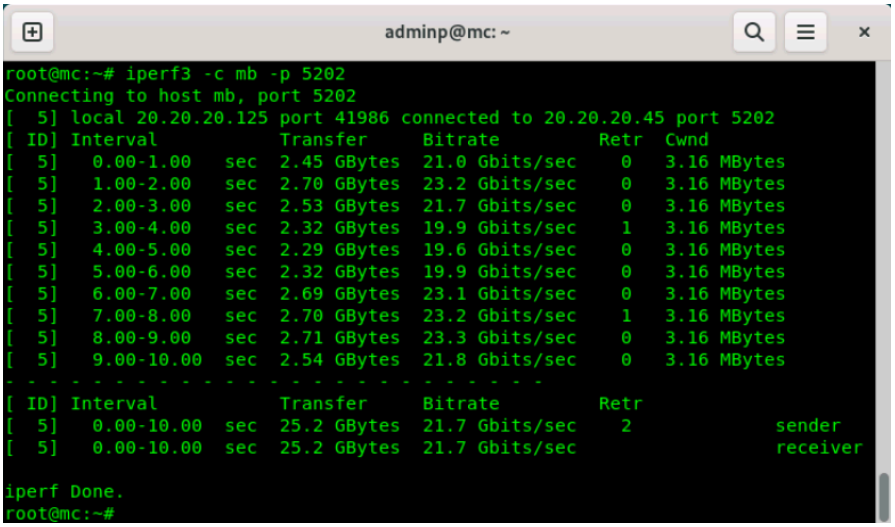


MVB (host)

A l'ordinador client, executem la comanda iperf3 -c mb -p 5202:

- paràmetre **-c** per indicar que com el client en aquesta connexió.
- **mb**, el nom del servidor que hem esmentat. Introduïm en aquest cas "mb", ja que la taula ARP ja configurada s'encarrega de dirigir-la a la ip de la màquina coneguda.

- paràmetre **-p** per a fer servir el port 5202



MVC (client)

D'aquesta execució es poden treure les conclusions següents:

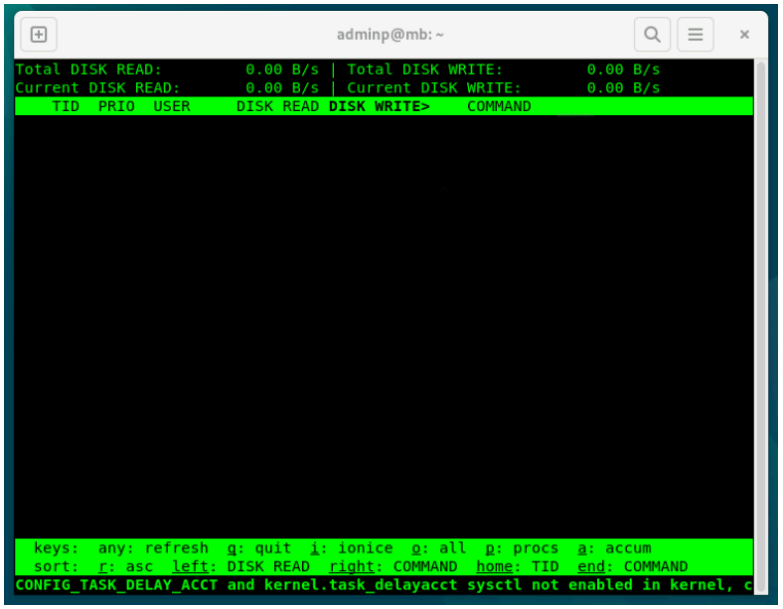
- La velocitat de transmissió de dades en la xarxa 20.20.20.0/23 és relativament **alta** (pel nostre criteri), amb una mitja de 2,52 GigaBytes per segon, i un bitrate de 21,7 Gigabits per segon. Calculem una desviació típica de 164 MB/s per la transferència de dades, i d'1,43 Gb/s pel bitrate, unes dades que considerem que indiquen unes velocitats bastant consistents. Aquestes dades aparellades ens indiquen una **bona i constant velocitat** de transmissió per la xarxa en condicions normals.

- Tal com ens indica la columna *Retr*, només en un parell d'ocasions s'ha hagut de retransmetre algun paquet degut a congestió o problemes amb el hardware. Considerem que amb tal quantitat d'informació enviada, aquest nombre d'errors és insignificant, i la poca presència d'aquests indiquen una **excel·lent qualitat de la xarxa** en condicions normals.

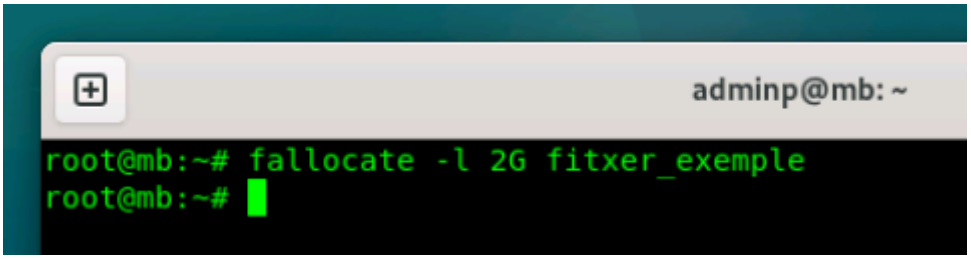
- La columna *Cwnd* ens indica una **bona configuració de TCP** en la xarxa, ja que la congestió només ha crescut fins a 3,16 MB en tota la transmissió.

Anàlisi amb iotop

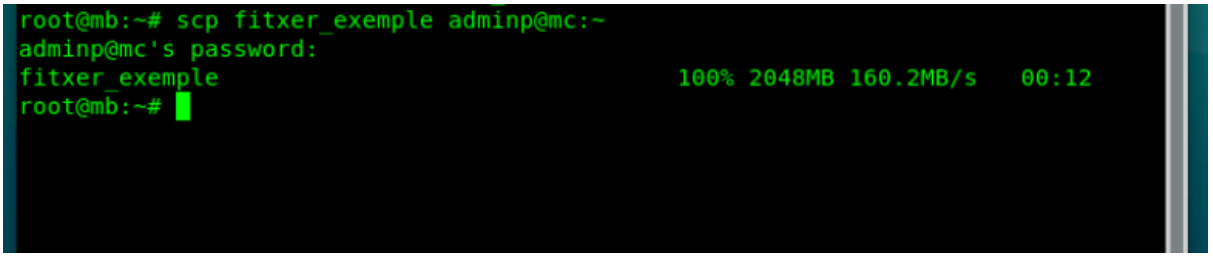
Aquesta prova consisteix en crear un arxiu real, enviar-lo entre màquines fent servir *scp* i analitzar el rendiment de la xarxa mentrestant. Els passos son els següents:



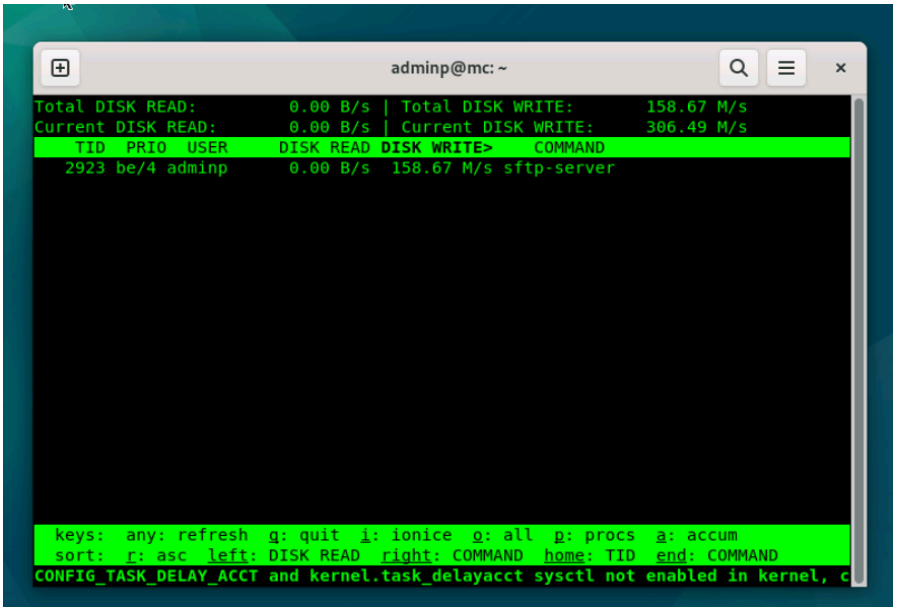
Abans de fer cap enviament, obrim el servei per l'anàlisi amb *iotop -o*



Creem l'arxiu amb *fallocate*



Enviem l'arxiu amb *scp*

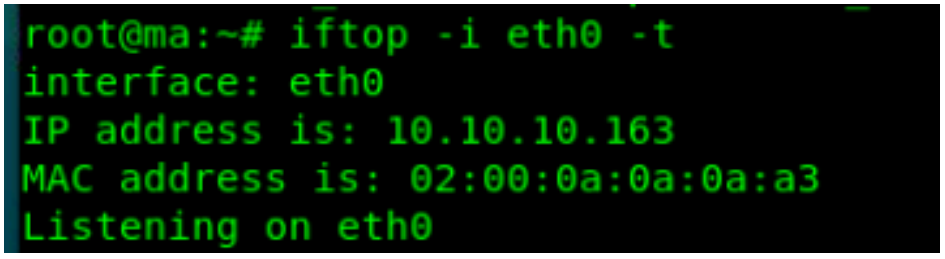


Analitzem la transferència amb la consolo que està executant iotop

Durant l'enviament de l'arxiu de 2 GB, observem velocitats d'una 160 MB/s amb poca variància, indicant un bon configuració estat de la xarxa. Veiem una clara diferència entre la prova anterior de *iperf3* (~2,5 GB/s) amb la de *scp*, això es pot deure a que *iperf3* només mesura **l'ample de banda**, mentre que *scp* inclou la càrrega extra de l'encriptació i la gestió de fitxers, cosa que redueix la velocitat.

Anàlisi amb iftop

Vam intentar instalar **ntopng**, però com no vam aconseguir fer-ho, ho vam fer amb una eina similar, **iftop**.
A la MVA, la qual té les dues interfícies, una per la xarxa 10.10.10.0/24 i una per 20.20.20.0/23, vam instalar iftop i vam executar la comanda:



interfície per la xarxa 10.10.10.0/24

```
                                                                              
   # Host name (port/service if enabled)            last 2s   last 10s   last 40s cumulative
--------------------------------------------------------------------------------------------
   1 255.255.255.255                        =>         0b        0b        0b         0B
     0.0.0.0                                <=      3.53Kb    2.64Kb    2.62Kb     4.59KB
   2 255.255.255.255                        =>         0b        0b        0b         0B
     10.90.90.90                            <=         0b       276b       197b       345B
   3 mva-gw.gixpd.org                       =>         0b        56b       242b       424B
     va-dalila.uab.cat                      <=         0b       102b       413b       723B
   4 192.168.11.104                         =>         0b        0b        41b        72B
     239.2.11.71                            <=         0b        0b         0b         0B
--------------------------------------------------------------------------------------------
Total send rate:                                       0b        56b       242b
Total receive rate:                                 3.53Kb    3.01Kb    3.26Kb
Total send and receive rate:                        3.53Kb    3.06Kb    3.49Kb
--------------------------------------------------------------------------------------------
Peak rate (sent/received/total):                    1.38Kb    4.16Kb    4.98Kb
Cumulative (sent/received/total):                     424B    5.70KB    6.11KB
============================================================================================

root@ma:~#
```

Ens va mostrar aquests resultats. Com es veu, hi ha poca activitat en la interfície externa (pocs Bytes o KB)

```
root@ma:~# iftop -i eth1 -t
interface: eth1
IP address is: 20.20.20.71
MAC address is: 02:00:14:14:14:47
Listening on eth1
```

Per la interfície interna eth1

```
                                                                              
   # Host name (port/service if enabled)            last 2s   last 10s   last 40s cumulative
--------------------------------------------------------------------------------------------
   1 mva.gixpd.org                          =>       904b      938b      781b      1.14KB
     mvb.gixpd.org                          <=       592b      640b      533b       800B
   2 mad07s23-in-f14.1e100.net              =>       672b      538b      448b       672B
     mvb.gixpd.org                          <=       672b      538b      448b       672B
--------------------------------------------------------------------------------------------
Total send rate:                                    1.54Kb    1.44Kb    1.20Kb
Total receive rate:                                 1.23Kb    1.15Kb     981b
Total send and receive rate:                        2.77Kb    2.59Kb    2.16Kb
--------------------------------------------------------------------------------------------
Peak rate (sent/received/total):                    2.15Kb    1.67Kb    3.82Kb
Cumulative (sent/received/total):                   1.80KB    1.44KB    3.24KB
============================================================================================

```

Al fer que la MVB faci un ping de google.com, s'observa activitat a la xarxa. Al fer només aquesta operació és normal que només s'observin uns pobs KB a la xarxa

Conclusions

Nagios

La implementació de Nagios com a eina de monitorització ha permès obtenir una visió detallada de l'estat dels hosts i serveis configurats. Després de completar el procés de configuració, es poden destacar els següents punts:

- Nagios ofereix una plataforma molt personalitzable que permet monitoritzar múltiples serveis, com ara ping, HTTP, SSH, i altres específics com l'ús del disc amb check_disk. Aquesta flexibilitat és molt útil per adaptar-se a necessitats concretes en entorns complexos.

- L'alerta configurada per detectar l'ús elevat del disc en els hosts monitoritzats va funcionar correctament. La detecció automàtica d'estats com CRITICAL o OK per l'ús del disc demostra que Nagios pot ajudar a prevenir problemes abans que tinguin un impacte negatiu. Tanmateix, els CRITICAL, OK i WARNING aplicaven a tots els serveis.

- Tot i que la interfície de Nagios no és moderna, proporciona una manera efectiva de visualitzar els estats dels hosts i serveis. Amb la configuració adequada, es poden gestionar fàcilment els elements monitoritzats des d'aquesta interfície.

En general, Nagios és una eina excel·lent per monitoritzar infraestructures locals o remotes amb configuracions específiques. No obstant això, la seva complexitat inicial pot requerir un període d'aprenentatge abans d'aprofitar completament les seves capacitats.

Netdata

La implementació de Netdata Cloud ha destacat per la seva senzillesa i capacitat d'oferir dades en temps real de manera visual i accessible des de qualsevol lloc. Les conclusions principals són:

- A diferència de Nagios, Netdata s'instal·la amb una sola comanda proporcionada per la plataforma. Aquest procés automatitzat simplifica la configuració i la integració dels nodes monitoritzats al sistema.

- Netdata ofereix una interfície moderna i interactiva que permet visualitzar mètriques detallades com l'ús de CPU, memòria, disc i tràfic de xarxa en temps real. Aquesta característica és especialment útil per identificar anomalies de manera ràpida.

- La possibilitat de gestionar múltiples nodes des d'una única plataforma basada en el núvol és un gran avantatge per a entorns amb múltiples màquines. Això elimina la necessitat de mantenir servidors locals o interfícies separades.

- Tot i la seva facilitat d'ús, Netdata pot ser menys flexible que Nagios per a escenaris on es requereixen alertes personalitzades o monitorització específica de serveis menys comuns.

En conclusió, Netdata Cloud és una eina ideal per a la monitorització ràpida i eficient d'entorns amb múltiples màquines, especialment per usuaris que necessiten visualització en temps real amb una configuració mínima. La seva integració al núvol el converteix en una opció excel·lent per a entorns dinàmics. No obstant això, pot no ser tan personalitzable com altres eines com Nagios.

---

iPerf3

L'ús d'iPerf3 ha demostrat que la xarxa interna entre MB i MC té un rendiment excel·lent, amb velocitats altes i poques pèrdues de paquets. La xarxa pot gestionar una gran quantitat de dades amb un bon rendiment i una mínima congestió, suggerint que el seu funcionament és eficient en condicions normals.

---

iotop

L'anàlisi amb iotop confirma que la transferència d'arxius mitjançant SCP té una velocitat de 160 MB/s, que és més baixa que amb iPerf3. Aquesta diferència es deu a l'impacte de l'encriptació i la gestió de fitxers en SCP, però les velocitats són encara bones, indicant que la xarxa està ben configurada, tot i la càrrega addicional d'aquesta eina.

---

iftop

L'ús d'iftop per monitoritzar la xarxa a la màquina MVA revela que la xarxa interna 20.20.20.0/23 té una activitat moderada durant les proves, amb poca activitat en la interfície externa. Els resultats són coherents amb les proves anteriors, suggerint que la xarxa interna funciona bé, amb un consum de dades relativament baix en operacions senzilles com el ping.