Part I

Monitoratge de registres LOG

Executar un terminal i visualitzar, en temps real, algun dels fitxers de registre del sistema. Veure unicament les noves insercions i indicar els arxius que heu trobat.

Arxius de registre més habituals (poden variar segons la distribució):

- /var/log/message: registre de missatges generals del sistema

```
root@user-VirtualBox:/home/user# less +F /var/log/dmesg
```

```
[   12.135778] kernel: Ais CIR mode byb optimization enabled
[   14.281469] kernel: snd_intel8x0 0000:00:05.0: white list rate for 1028:0177 is 48000
[   18.027924] kernel: audit: type=1400 audit(1614762860.388:2): apparmor="STATUS" operation="profile_load" profile="unconfined" name="lsb_relea
se" pid=513 comm="apparmor_parser"
[   18.790353] kernel: audit: type=1400 audit(1614762860.548:3): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/
snapd/snap-confine" pid=515 comm="apparmor_parser"
[   18.790363] kernel: audit: type=1400 audit(1614762860.548:4): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/
snapd/snap-confine//mount-namespace-capture-helper" pid=515 comm="apparmor_parser"
[   18.829696] kernel: audit: type=1400 audit(1614762860.584:5): apparmor="STATUS" operation="profile_load" profile="unconfined" name="ippusbxd"
pid=516 comm="apparmor_parser"
[   18.858943] kernel: audit: type=1400 audit(1614762860.616:6): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/lib/
cups/backend/cups-pdf" pid=514 comm="apparmor_parser"
[   18.858950] kernel: audit: type=1400 audit(1614762860.616:7): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin
/cupsd" pid=514 comm="apparmor_parser"
[   18.858953] kernel: audit: type=1400 audit(1614762860.616:8): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin
/cupsd//third_party" pid=514 comm="apparmor_parser"
[   18.885906] kernel: audit: type=1400 audit(1614762860.644:9): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/usr/sbin
/cups-browsed" pid=518 comm="apparmor_parser"
[   18.959490] kernel: audit: type=1400 audit(1614762860.716:10): apparmor="STATUS" operation="profile_load" profile="unconfined" name="nvidia_m
odprobe" pid=521 comm="apparmor_parser"
[   18.959498] kernel: audit: type=1400 audit(1614762860.716:11): apparmor="STATUS" operation="profile_load" profile="unconfined" name="nvidia_m
odprobe//kmod" pid=521 comm="apparmor_parser"
[   25.379377] kernel: kauditd_printk_skb: 19 callbacks suppressed
[   25.379380] kernel: audit: type=1400 audit(1614762867.136:31): apparmor="DENIED" operation="capable" profile="/usr/sbin/cups-browsed" pid=658
 comm="cups-browsed" capability=23  capname="sys_nice"
Waiting for data... (interrupt to abort)
```

- /var/log/auth.log: log d'autenticació

```
root@user-VirtualBox:/home/user# less +F /var/log/auth.log
```

```
~
~
~
~
Mar  2 13:39:36 user-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Mar  2 13:39:36 user-VirtualBox pkexec[5772]: user: Executing command [USER=root] [TTY=unknown] [CWD=/home/user] [COMMAND=/usr/lib/update-notifi
er/package-system-locked]
Mar  3 10:14:24 user-VirtualBox systemd-logind[593]: New seat seat0.
Mar  3 10:14:24 user-VirtualBox systemd-logind[593]: Watching system buttons on /dev/input/event0 (Power Button)
Mar  3 10:14:24 user-VirtualBox systemd-logind[593]: Watching system buttons on /dev/input/event1 (Sleep Button)
Mar  3 10:14:24 user-VirtualBox systemd-logind[593]: Watching system buttons on /dev/input/event2 (AT Translated Set 2 keyboard)
Mar  3 10:17:04 user-VirtualBox CRON[870]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  3 10:17:04 user-VirtualBox CRON[870]: pam_unix(cron:session): session closed for user root
Mar  3 10:17:57 user-VirtualBox useradd[880]: failed adding user 'vboxadd', data deleted
Mar  3 10:17:57 user-VirtualBox useradd[881]: failed adding user 'vboxadd', data deleted
Mar  3 10:18:09 user-VirtualBox gdm-autologin]: gkr-pam: no password is available for user
Mar  3 10:18:16 user-VirtualBox gdm-autologin]: pam_unix(gdm-autologin:session): session opened for user user by (uid=0)
Mar  3 10:18:16 user-VirtualBox systemd-logind[593]: New session 2 of user user.
Mar  3 10:18:17 user-VirtualBox systemd: pam_unix(systemd-user:session): session opened for user user by (uid=0)
Mar  3 10:18:23 user-VirtualBox gdm-autologin]: gkr-pam: gnome-keyring-daemon started properly
Mar  3 10:19:15 user-VirtualBox dbus-daemon[551]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
Mar  3 10:19:31 user-VirtualBox gnome-keyring-daemon[1023]: The Secret Service was already initialized
Mar  3 10:19:31 user-VirtualBox gnome-keyring-daemon[1023]: The PKCS#11 component was already initialized
Mar  3 10:20:51 user-VirtualBox polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.48 [/usr/bin/gn
ome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale es_ES.UTF-8)
Mar  3 10:22:18 user-VirtualBox pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Mar  3 10:22:18 user-VirtualBox pkexec[2585]: user: Executing command [USER=root] [TTY=unknown] [CWD=/home/user] [COMMAND=/usr/lib/update-notifi
er/package-system-locked]
Mar  3 10:23:38 user-VirtualBox sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No existe el archivo o el directorio
Mar  3 10:23:40 user-VirtualBox sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No existe el archivo o el directorio
Mar  3 10:23:40 user-VirtualBox sudo:    user : TTY=pts/0 ; PWD=/home/user ; USER=root ; COMMAND=/usr/bin/su
Mar  3 10:23:40 user-VirtualBox sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar  3 10:23:40 user-VirtualBox su: (to root) user on pts/0
Mar  3 10:23:40 user-VirtualBox su: pam_unix(su:session): session opened for user root by (uid=0)
Mar  3 10:30:02 user-VirtualBox CRON[3263]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar  3 10:30:02 user-VirtualBox CRON[3263]: pam_unix(cron:session): session closed for user root
Waiting for data... (interrupt to abort)
```

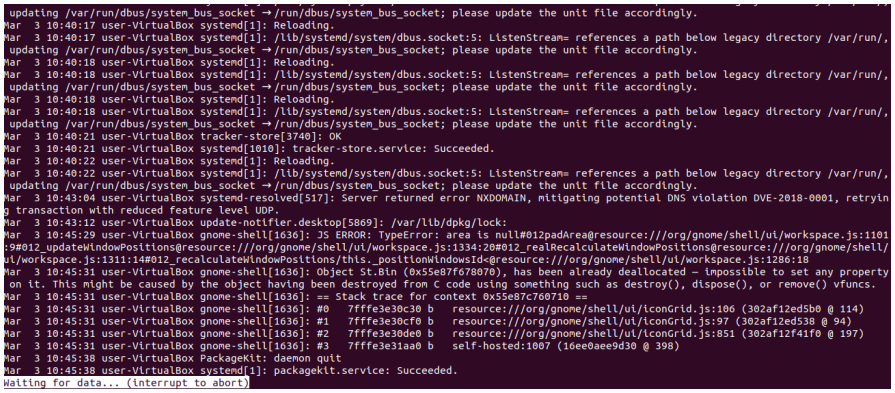
- /var/log/kern.log: registre del kernel

```
root@user-VirtualBox:/home/user# less +F /var/log/kern.log
```

```
info="same as current profile, skipping" profile="unconfined" name="/snap/snapd/11036/usr/lib/snapd/snap-confine" pid=2785 comm="apparmor_parser
"
Mar  3 10:23:36 user-VirtualBox kernel: [  572.934272] audit: type=1400 audit(1614763416.591:45): apparmor="STATUS" operation="profile_replace"
info="same as current profile, skipping" profile="unconfined" name="/snap/snapd/11036/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
" pid=2785 comm="apparmor_parser"
Mar  3 10:23:37 user-VirtualBox kernel: [  573.886748] audit: type=1400 audit(1614763417.543:46): apparmor="STATUS" operation="profile_load" pro
file="unconfined" name="snap.snap-store.hook.configure" pid=2788 comm="apparmor_parser"
Mar  3 10:23:38 user-VirtualBox kernel: [  574.368425] audit: type=1400 audit(1614763418.023:47): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap-update-ns.snap-store" pid=2787 comm="apparmor_parser"
Mar  3 10:23:39 user-VirtualBox kernel: [  575.641977] audit: type=1400 audit(1614763419.300:48): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.snap-store" pid=2792 comm="apparmor_parser"
Mar  3 10:23:39 user-VirtualBox kernel: [  575.745239] audit: type=1400 audit(1614763419.404:49): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.ubuntu-software" pid=2793 comm="apparmor_parser"
Mar  3 10:23:40 user-VirtualBox kernel: [  576.427374] audit: type=1400 audit(1614763420.084:50): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=2794 comm="apparmor_parser"
Mar  3 10:23:50 user-VirtualBox kernel: [  587.078309] audit: type=1400 audit(1614763430.740:51): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.hook.configure" pid=2812 comm="apparmor_parser"
Mar  3 10:23:51 user-VirtualBox kernel: [  587.945747] audit: type=1400 audit(1614763431.608:52): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.snap-store" pid=2813 comm="apparmor_parser"
Mar  3 10:23:51 user-VirtualBox kernel: [  588.050649] audit: type=1400 audit(1614763431.712:53): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap-update-ns.snap-store" pid=2811 comm="apparmor_parser"
Mar  3 10:23:52 user-VirtualBox kernel: [  588.809745] audit: type=1400 audit(1614763432.472:54): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.ubuntu-software" pid=2814 comm="apparmor_parser"
Mar  3 10:23:52 user-VirtualBox kernel: [  588.924477] audit: type=1400 audit(1614763432.584:55): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=2815 comm="apparmor_parser"
Mar  3 10:27:22 user-VirtualBox kernel: [  798.704577] audit: type=1400 audit(1614763642.204:56): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.hook.configure" pid=3020 comm="apparmor_parser"
Mar  3 10:27:22 user-VirtualBox kernel: [  799.211944] audit: type=1400 audit(1614763642.712:57): apparmor="STATUS" operation="profile_replace"
info="same as current profile, skipping" profile="unconfined" name="snap-update-ns.snap-store" pid=3019 comm="apparmor_parser"
Mar  3 10:27:23 user-VirtualBox kernel: [  799.963400] audit: type=1400 audit(1614763643.460:58): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.snap-store" pid=3021 comm="apparmor_parser"
Mar  3 10:27:23 user-VirtualBox kernel: [  800.099035] audit: type=1400 audit(1614763643.596:59): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.ubuntu-software" pid=3022 comm="apparmor_parser"
Mar  3 10:27:24 user-VirtualBox kernel: [  800.752915] audit: type=1400 audit(1614763644.249:60): apparmor="STATUS" operation="profile_replace"
profile="unconfined" name="snap.snap-store.ubuntu-software-local-file" pid=3023 comm="apparmor_parser"
Waiting for data... (interrupt to abort)
```

- /var/log/cron.log: registre de crond

```
root@user-VirtualBox:/home/user# less +F /var/log/syslog
```



- /var/log/maillog: registre del servidor de mails

  No existeix

- /var/log/qmail/ : registre de Qmail

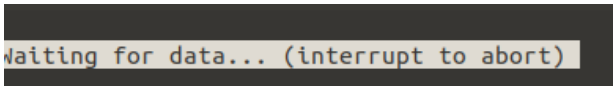
  No existeix

- /var/log/httpd/: registre d'errors i accés a Apache

  No existeix

- /var/log/lighttpd: registre d'errors i accés a Lighttpd

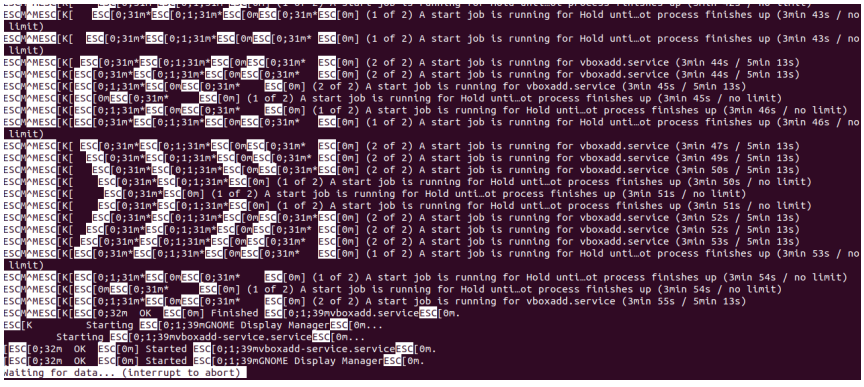
```
root@userver2021:/home/vib01# less +F /var/log/lightdm/lightdm.log
```



Està buit per que no he tocat lighttpd

- /var/log/boot.log : registre d'inici del sistema
(al estar en binari no es pot mostrar correctament)

```
root@user-VirtualBox:/home/user# less +F /var/log/boot.log
```



- /var/log/mysqld.log: registre de la base de dades MySQL

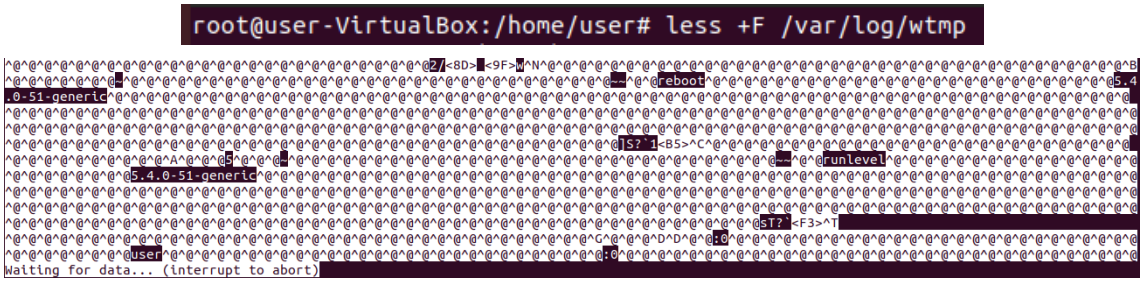
  No existeix

- /var/log/secure: log d'autenticació

  No existeix

- /var/log/utmp or /var/log/wtmp : registre de logins

  (al estar en binari no es pot mostrar correctament)

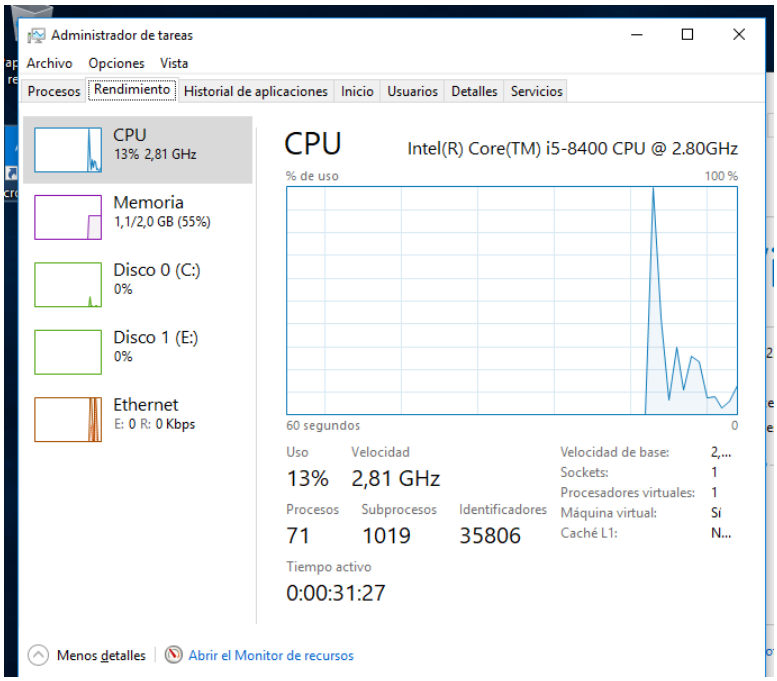


Part II:

Rendiment:

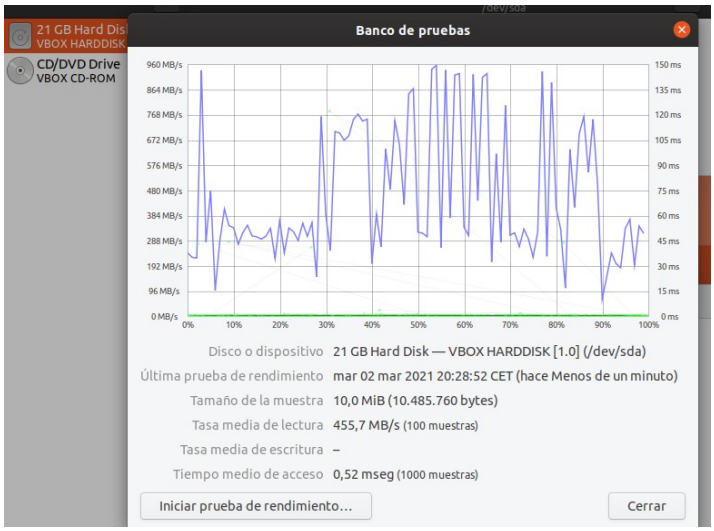
Windows:

Amb les eines que proporciona Windows 10, analitzar les característiques del vostre sistema segons processos, cpu, discs...



Linux:

En el cas de l'Ubuntu incorpora una eina per analitzar el rendiment dels discos. Per accedir a aquesta eina. amb l'opció cerca busqueu "Discs" i en "Més accions" seleccioneu "Test de referència". Analitzeu també les característiques més remarcables.



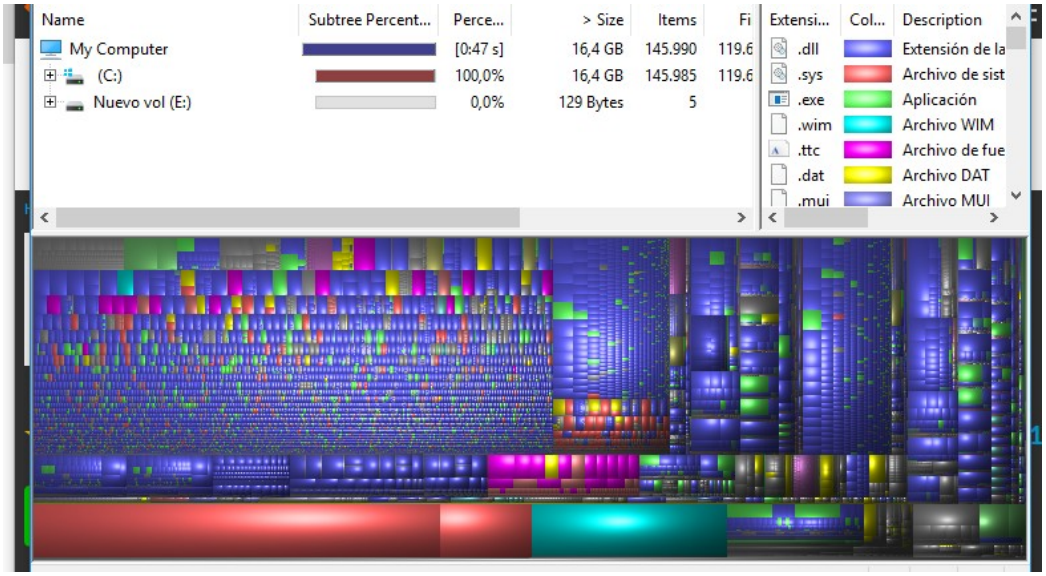
Estadístiques:

windows

Analitzar les característiques més remarcables del programari d'estadístiques, amb llicència GPLv2, Windirstat

http://sourceforge.net/projects/windirstat/

Permet visualitzar l'us del disc dur. Veus amb blocs l'us de memòria, també la memòria total, veure programa per programa cuant casta de memòria, i altres funcions..



Linux

En el cas d'Ubuntu es disposa de l'eina "Baobab" o analitzador de l'ús dels discs. Analitzeu també les característiques més remarcables.