

UNIDAD DIDÁCTICA 5 - CUESTIONES V

1. Detalla los campos que se guardan en el fichero `/etc/fstab` para cada uno de los discos o particiones del sistema. ¿Qué contiene el fichero `/etc/fstab` de tu máquina? Interpreta cada línea y cada campo de éstas. ¿Qué indica el primer campo de una línea del `fstab` que tenga el valor `"sdb2"`?

Lo más destacado de este fichero es la lista de discos y particiones disponibles. En ella se indica cómo montar cada dispositivo y qué configuración utilizar.

En el fichero `fstab` de mi máquina virtual, se encuentra lo siguiente:

```
luque@serverluque:/etc$ cat fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
/dev/disk/by-uuid/641933db-ccae-498f-9d20-8e8c8ec0b953 none swap sw 0 0
# / was on /dev/sda4 during curtin installation
/dev/disk/by-uuid/74bcfde5-12af-4ac3-8a43-38c06f552e96 / ext4 defaults 0 1
# /home was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/cf175c9a-6bf8-4d82-b431-548eb6e7a73b /home ext4 defaults 0 1
/swap.img none swap sw 0 0
luque@serverluque:/etc$

luque@serverluque:/etc$ blkid
/dev/sda4: UUID="74bcfde5-12af-4ac3-8a43-38c06f552e96" BLOCK_SIZE="4096" TYPE="ext4" PARTUUID="80d9
971-272e-4c93-a6f3-24d672b108ac"
/dev/sda2: UUID="cf175c9a-6bf8-4d82-b431-548eb6e7a73b" BLOCK_SIZE="4096" TYPE="ext4" PARTUUID="8e05
626-8a94-489d-a548-906831e6f438"
/dev/sda3: UUID="641933db-ccae-498f-9d20-8e8c8ec0b953" TYPE="swap" PARTUUID="14a3fc9e-033e-4131-825
-d21c4513cb88"
luque@serverluque:/etc$ _
```

Que tenga el valor `sdb2`, significa que dispone del segundo disco SCSI en cuanto a su dirección.

Campos:

`/dev/sda2`: Directorio lógico que hace referencia a una partición o disco.

`/home`: Directorio donde será montado el dispositivo físico.

`ext4`: Tipo de sistema de archivos que usará el dispositivo.

`dump (0)`: Indica si debe hacer o no el backup, en este caso no.

`pass (1)`: Indica el orden en el que `fsck` examinará la partición en busca de errores, en este caso, máxima prioridad.

2. ¿Cómo está organizado el sistema de registros de Ubuntu Server? Directorio, ficheros, formato de mensajes, proceso gestor de registros,

UNIDAD DIDÁCTICA 5 - CUESTIONES V

limpieza de registros antiguos, ... ¿Cuáles son los principales ficheros de registro (log)? ¿Es posible que una aplicación tenga su propio fichero de registro?

Existen muchos tipos de ficheros de registros o logs, estos pueden encontrarse usualmente en /var/log.

Entre estos, se hallan los siguientes:

- syslog: generales del sistema, por ejemplo, asignación de IP por el servicio DHCP.
- kern.log: del kernel
- auth.log: intentos de acceso al sistema (correctos o no)
- dpkg.log: información sobre los paquetes que se instalan y desinstalan.

Algunas aplicaciones pueden tener sus propios registros, lo que hace que puedan controlarse por sí mismas en cierta manera.

- <programa>.log: algunos programas tienen su propio log y no usan el general syslog.

Para evitar la sobrecarga de información que pueden generar los logs, tenemos un fichero llamado logrotate (rotación de registros) que puede ser configurado para llevar a cabo dicha labor.

Además, podemos configurar todos los logs con el journalctl simultáneamente.

3. Realiza las siguientes tareas y busca en el sistema de registro los eventos correspondientes:

a. desactivar y activar la tarjeta de red

Para hacerlo, usaremos el comando `ifconfig eth0 down`, y para reactivar la interfaz, usaremos el comando `ifconfig eth0 up`.

Sin embargo, no lo he podido realizar en mi máquina puesto que no me deja instalar el paquete net-tools de ninguna manera, por lo que no tengo acceso al comando `ifconfig`.

UNIDAD DIDÁCTICA 5 - CUESTIONES V

```
root@serverluque:/etc# ifconfig eth0 down
Command 'ifconfig' not found, but can be installed with:
apt install net-tools
root@serverluque:/etc# _
```

```
Err:1 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Temporary failure resolving 'es.archive.ubuntu.com'
Err:2 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease
Temporary failure resolving 'es.archive.ubuntu.com'
Err:3 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Temporary failure resolving 'es.archive.ubuntu.com'
Err:4 http://es.archive.ubuntu.com/ubuntu jammy-security InRelease
Temporary failure resolving 'es.archive.ubuntu.com'
Reading package lists... Done
W: Failed to fetch http://es.archive.ubuntu.com/ubuntu/dists/jammy/InRelease Temporary failure res
lving 'es.archive.ubuntu.com'
W: Failed to fetch http://es.archive.ubuntu.com/ubuntu/dists/jammy-updates/InRelease Temporary fail
ure resolving 'es.archive.ubuntu.com'
W: Failed to fetch http://es.archive.ubuntu.com/ubuntu/dists/jammy-backports/InRelease Temporary fa
ilure resolving 'es.archive.ubuntu.com'
W: Failed to fetch http://es.archive.ubuntu.com/ubuntu/dists/jammy-security/InRelease Temporary fai
lure resolving 'es.archive.ubuntu.com'
W: Some index files failed to download. They have been ignored, or old ones used instead.
root@serverluque:/etc# ifconfig eth0 down
```

b. instalar la aplicación Wireshark

```
root@serverluque:/etc# add-apt-repository ppa:wireshark-dev/stable
```

```
root@serverluque:/etc# apt install wireshark
```

UNIDAD DIDÁCTICA 5 - CUESTIONES V

```
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/s/spandsp/libspandsp2_0.0.6%2fsg-2_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/main/s/speex/libspeexdsp1_1.2%7erc1.2-1ubuntu3_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/main/libs/libssh/libssh-gcrypt-4_0.9.6build1_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/main/libw/libwacom/libwacom-bin_2.2.0-amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/w/wireshark/libwireshark-data_6.2-2_all.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/main/c/c-ares/libc-ares2_1.18.1-1buildamd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/main/s/sbc/libsbcl1.5-3build2_amd64.dTemporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/main/s/snappy/libsnappy1v5_1.1.8-1builamd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/w/wireshark/libwsutil13_3.6.2_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/w/wireshark/libwiretap12_3.6.2_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/w/wireshark/libwireshark15_3.2-2_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/main/m/mesa/mesa-vulkan-drivers_22.0.5ubuntu0.1_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/q/qtbase-opensource-src/qt5-g-platformtheme_5.15.3%2bdfsg-2ubuntu0.1_amd64.deb Temporary failure resolving 'es.archive.ubuntu.m'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/q/qttranslations-opensource-s/qttranslations5-110n_5.15.3-1_all.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/w/wireshark/wireshark-common_6.2-2_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/w/wireshark/wireshark-qt_3.6.2_amd64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Failed to fetch http://es.archive.ubuntu.com/ubuntu/pool/universe/w/wireshark/wireshark_3.6.2-2md64.deb Temporary failure resolving 'es.archive.ubuntu.com'
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
root@serverluque:/etc# _
```

Tras probar varias veces y de varias formas (añadiendo el repositorio a la máquina, usando el apt install wireshark, probando el --fix-missing para solucionar el error, no he podido descargar la aplicación wireshark.)

c. Crearte un usuario y acceder con él

UNIDAD DIDÁCTICA 5 - CUESTIONES V

```
apt install net-tools
root@serverluque:/etc# adduser hugo
Adding user `hugo' ...
Adding new group `hugo' (1001) ...
Adding new user `hugo' (1001) with group `hugo' ...
Creating home directory `/home/hugo' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for hugo
Enter the new value, or press ENTER for the default
  Full Name []: Hugo
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@serverluque:/etc#
```

```
Is the information correct? [Y/n] y
root@serverluque:/etc# login hugo
Password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux
```

```
hugo@serverluque:~$ _
```

d. Cerrar la sesión de ese usuario y provocar un error “Contraseña Incorrecta”

```
hugo@serverluque:~$ exit
logout
root@serverluque:/etc#
```

```
root@serverluque:/etc# login hugo
Password:

Login incorrect
serverluque login: _
```

4. El comando `journalctl` es capaz de obtener información de todos los ficheros de registros y mostrarlos en un único listado. Busca información sobre sus opciones de ejecución y muestra:

a. los logs del último arranque del sistema

```
luque@serverluque:/etc$ journalctl -b -1
```


UNIDAD DIDÁCTICA 5 - CUESTIONES V

```
Nov 30 10:56:28 serverluque kernel: Linux version 5.15.0-43-generic (buildd@lcy02-amd64-076) (gcc (buildd@lcy02-amd64-076) 12.2.0, GNU ld (GNU) 2.35.2) root=UUID=7b1c0200-4b56-4d01-b000-000000000000 ro=initrd=initrd.img-5.15.0-43-generic root=UUID=7b1c0200-4b56-4d01-b000-000000000000
Nov 30 10:56:28 serverluque kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-43-generic root=UUID=7b1c0200-4b56-4d01-b000-000000000000 ro=initrd=initrd.img-5.15.0-43-generic root=UUID=7b1c0200-4b56-4d01-b000-000000000000
Nov 30 10:56:28 serverluque kernel: KERNEL supported cpus:
Nov 30 10:56:28 serverluque kernel:   Intel GenuineIntel
Nov 30 10:56:28 serverluque kernel:   AMD AuthenticAMD
Nov 30 10:56:28 serverluque kernel:   Hygon HygonGenuine
Nov 30 10:56:28 serverluque kernel:   Centaur CentaurHauls
Nov 30 10:56:28 serverluque kernel:   zhaoxin Shanghai
Nov 30 10:56:28 serverluque kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Nov 30 10:56:28 serverluque kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Nov 30 10:56:28 serverluque kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Nov 30 10:56:28 serverluque kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Nov 30 10:56:28 serverluque kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, default xstate_size is 200
Nov 30 10:56:28 serverluque kernel: signal: max sigframe size: 1776
Nov 30 10:56:28 serverluque kernel: BIOS-provided physical RAM map:
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbf] usable
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x0000000000009fc0-0x0000000000009fff] reserved
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x000000000000f000-0x000000000000ffff] reserved
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x0000000001000000-0x0000000007ffefff] usable
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x0000000007fff000-0x0000000007ffffff] ACPI data
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Nov 30 10:56:28 serverluque kernel: NX (Execute Disable) protection: active
Nov 30 10:56:28 serverluque kernel: SMBIOS 2.5 present.
Nov 30 10:56:28 serverluque kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2019
Nov 30 10:56:28 serverluque kernel: Hypervisor detected: KVM
Nov 30 10:56:28 serverluque kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Nov 30 10:56:28 serverluque kernel: kvm-clock: cpu 0, msr 70801001, primary cpu clock
Nov 30 10:56:28 serverluque kernel: kvm-clock: using sched offset of 8154335338 cycles
Nov 30 10:56:28 serverluque kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1400000000000000 max_idle_ns: 440795328200 ns
Nov 30 10:56:28 serverluque kernel: tsc: Detected 3292.394 MHz processor
Nov 30 10:56:28 serverluque kernel: e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
Nov 30 10:56:28 serverluque kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
Nov 30 10:56:28 serverluque kernel: last_pfn = 0x7fff0 max_arch_pfn = 0x400000000
Nov 30 10:56:28 serverluque kernel: Disabled
```

lines 1-36

Activar Windows

b. los últimos 30 mensajes.

UNIDAD DIDÁCTICA 5 - CUESTIONES V

```
luque@serverluque:/etc$ journalctl -n 30
Nov 30 12:28:36 serverluque systemd[1]: Starting Time & Date Service...
Nov 30 12:28:36 serverluque dbus-daemon[614]: [system] Successfully activated service 'org.freedesktop.timedated'
Nov 30 12:28:36 serverluque systemd[1]: Started Time & Date Service.
Nov 30 12:29:06 serverluque systemd[1]: systemd-timedated.service: Deactivated successfully.
Nov 30 12:29:06 serverluque dbus-daemon[614]: [system] Activating via systemd: service name='org.freedesktop.timedated'
Nov 30 12:29:06 serverluque systemd[1]: Starting Time & Date Service...
Nov 30 12:29:06 serverluque dbus-daemon[614]: [system] Successfully activated service 'org.freedesktop.timedated'
Nov 30 12:29:06 serverluque systemd[1]: Started Time & Date Service.
Nov 30 12:29:36 serverluque systemd[1]: systemd-timedated.service: Deactivated successfully.
Nov 30 12:29:36 serverluque dbus-daemon[614]: [system] Activating via systemd: service name='org.freedesktop.timedated'
Nov 30 12:29:36 serverluque systemd[1]: Starting Time & Date Service...
Nov 30 12:29:37 serverluque dbus-daemon[614]: [system] Successfully activated service 'org.freedesktop.timedated'
Nov 30 12:29:37 serverluque systemd[1]: Started Time & Date Service.
Nov 30 12:30:07 serverluque systemd[1]: systemd-timedated.service: Deactivated successfully.
Nov 30 12:30:07 serverluque dbus-daemon[614]: [system] Activating via systemd: service name='org.freedesktop.timedated'
Nov 30 12:30:07 serverluque systemd[1]: Starting Time & Date Service...
Nov 30 12:30:07 serverluque dbus-daemon[614]: [system] Successfully activated service 'org.freedesktop.timedated'
Nov 30 12:30:07 serverluque systemd[1]: Started Time & Date Service.
Nov 30 12:30:29 serverluque snapd[625]: devicemgr.go:1927: no NTP sync after 10m0s, trying auto-retry
Nov 30 12:30:37 serverluque systemd[1]: systemd-timedated.service: Deactivated successfully.
Nov 30 12:35:04 serverluque systemd[1]: Starting Cleanup of Temporary Directories...
Nov 30 12:35:04 serverluque systemd[1]: systemd-tmpfiles-clean.service: Deactivated successfully.
Nov 30 12:35:04 serverluque systemd[1]: Finished Cleanup of Temporary Directories.
Nov 30 12:47:50 serverluque audit[1058]: AVC apparmor="DENIED" operation="file_inherit" profile="m
Nov 30 12:47:50 serverluque kernel: kauditd_printk_skb: 19 callbacks suppressed
Nov 30 12:47:50 serverluque kernel: audit: type=1400 audit(1669812470.683:31): apparmor="DENIED" op
Nov 30 12:47:50 serverluque audit[1059]: AVC apparmor="DENIED" operation="file_inherit" profile="m
Nov 30 12:47:50 serverluque kernel: audit: type=1400 audit(1669812470.691:32): apparmor="DENIED" op
Nov 30 12:47:50 serverluque audit[1067]: AVC apparmor="DENIED" operation="file_inherit" profile="m
Nov 30 12:47:50 serverluque kernel: audit: type=1400 audit(1669812470.715:33): apparmor="DENIED" op
lines 1-30/30 (END)
```

c. la información desde hace dos días.

```
luque@serverluque:/etc$ journalctl --since "2022-11-28"
```


UNIDAD DIDÁCTICA 5 - CUESTIONES V

```
Nov 30 10:56:28 serverluque kernel: Linux version 5.15.0-43-generic (build@lcy02-amd64-076) (gcc
Nov 30 10:56:28 serverluque kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-43-generic root
Nov 30 10:56:28 serverluque kernel: KERNEL supported cpus:
Nov 30 10:56:28 serverluque kernel:   Intel GenuineIntel
Nov 30 10:56:28 serverluque kernel:   AMD AuthenticAMD
Nov 30 10:56:28 serverluque kernel:   Hygon HygonGenuine
Nov 30 10:56:28 serverluque kernel:   Centaur CentaurHauls
Nov 30 10:56:28 serverluque kernel:   zhaoxin   Shanghai
Nov 30 10:56:28 serverluque kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point
Nov 30 10:56:28 serverluque kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Nov 30 10:56:28 serverluque kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Nov 30 10:56:28 serverluque kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Nov 30 10:56:28 serverluque kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 byt
Nov 30 10:56:28 serverluque kernel: signal: max sigframe size: 1776
Nov 30 10:56:28 serverluque kernel: BIOS-provided physical RAM map:
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbfff] usable
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009fffff] reserv
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserv
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000007fffffff] usable
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x00000000007ffff000-0x00000000007fffffff] ACPI d
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserv
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserv
Nov 30 10:56:28 serverluque kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserv
Nov 30 10:56:28 serverluque kernel: NX (Execute Disable) protection: active
Nov 30 10:56:28 serverluque kernel: SMBIOS 2.5 present.
Nov 30 10:56:28 serverluque kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/0
Nov 30 10:56:28 serverluque kernel: Hypervisor detected: KVM
Nov 30 10:56:28 serverluque kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Nov 30 10:56:28 serverluque kernel: kvm-clock: cpu 0, msr 70801001, primary cpu clock
Nov 30 10:56:28 serverluque kernel: kvm-clock: using sched offset of 8154335338 cycles
Nov 30 10:56:28 serverluque kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles:
Nov 30 10:56:28 serverluque kernel: tsc: Detected 3292.394 MHz processor
Nov 30 10:56:28 serverluque kernel: e820: update [mem 0x00000000-0x000000ffff] usable ==> reserved
Nov 30 10:56:28 serverluque kernel: e820: remove [mem 0x000a0000-0x0000ffff] usable
Nov 30 10:56:28 serverluque kernel: last_pfn = 0x7ffff0 max_arch_pfn = 0x400000000
Nov 30 10:56:28 serverluque kernel: Disabled
```

d. la información generada por la aplicación WireShark

No he podido capturar la información generada por wireshark puesto que no he podido instalar dicha aplicación, como ya he explicado anteriormente en el ejercicio de instalación.