

FSO

PRÀCTICA 1

Antonio Torres Cabero
Eduard Bel
Cristina Izquierdo Lozano

Índex

Enunciat resumit	2
Importació	2
Filtratge de registres	2
Pseudocodi de les funcions	4
buscaMes()	4
buscaData()	4
buscaMaquina()	4
buscaProces()	5
neteja()	5
buscaPID()	5
buscaTots()	5
acabar()	6
exportaFiltrats()	6
comprovaLogs()	6
comprova_data()	8
Funcions i mètodes	9
Descodificació	9
Llibreria chardet	9
Mètode decode()	9
Joc de proves	10
Bàsica	10
Comprimida	16
Errònia	16

Enunciat resumit

L'objectiu és llegir fitxers de log i guardar les dades a una base de dades per tal de facilitar l'anàlisi de seguretat. Per a dur a terme això, es farà un programa en python3 tenint en compte diverses codificacions, parts binàries i compressions dels fitxers.

Input de l'usuari (en tkinter): fitxer de log a tractar i fitxer BD on guardar el resultat

Interfície gràfica: consultes de l'usuari

Condicions:

- fitxer DB existeix: nous registres s'afegeixen sense tenir en compte la possibilitat de que ja hi fossin.
- fitxer DB no existeix: es crea un de nou "_ddmmaa"

Output: missatge amb el path, nom del fitxer i els permisos d'accés

Importació

Formats:

1. 7 camps → mes dia hora nom-maquina dimoni[PID]: missatge
2. 6 camps → mes dia hora nom-maquina proces: missatge

Comprovacions: la línia ha de tenir aquest format i cada camp ha de tenir també el format esperat per a poder ser inserit a la BD. Si no, es descarta i s'avisava amb el stderr.

Simplificacions:

- BD no relacional, sense cap camp clau ni cap restricció. Podria arribar a haver-hi registres duplicats.
- Per inserir els missatges a la BD alguns caràcters poden trencar la sintaxi SQL → tractar-los com a URLs.

Filtratge de registres

Funcions de botons:

- **Mes** → filtrar els registres de la BD que el seu mes sigui el que l'usuari hagi escrit al camp *Cerca*.
 - *Comprovacions:* format correcte.
 - *Resultats:*
 - Listbox corresponent per tal que es mostrin a la GUI. El format usat serà exactament el del fitxer de log.
 - Actualitzar la *línia d'estat* mostrant quants elements s'han trobat que compleixin el criteri del query.
- **Tots** → mostrar tots els registres de la BD
- **Exporta** → mostrar tots els registres pel stdout amb el format inicial dels logs.

Exemple de comanda sobre la BD: sqlcmd="SELECT camp2,camp3 FROM taula WHERE camp1 LIKE '%buscat%'"

Pseudocodi de les funcions

buscaMes()

```
funcio buscaMes()  
mes_par := llegir();  
mostra := executar("SELECCIONAR esdeveniments on mes := mes_par);  
    j := 0;  
    per cada i en mostra fer  
        listBox := insertar(i);  
        j := j + 1;  
    fi per  
    estat := escriure("Elements filtrats: " + string(j));  
fi funcio
```

buscaData()

```
funcio buscaData()  
dia_par := llegir();  
mostra := executar("SELECCIONAR esdeveniments on dia := dia_par);  
    j := 0;  
    per cada i en mostra fer  
        listBox := insertar(i);  
        j := j + 1;  
    fi per  
    estat := escriure("Elements filtrats: " + string(j));  
fi funcio
```

buscaMaquina()

```
funcio buscaMaquina()  
    maquina_par := llegir();  
    mostra := executar("SELECCIONAR esdeveniments on maquina :=  
maquina_par);  
    j := 0;  
    per cada i en mostra fer  
        listBox := insertar(i);  
        j := j + 1;  
    fi per
```

```
    estat := escriure("Elements filtrats: " + string(j));  
fi funcio
```

buscaProces()

```
funcio buscaProces()  
    proces_par := llegir();  
    mostra := executar("SELECCIONAR esdeveniments on proces :=  
proces_par);  
    j := 0;  
    per cada i en mostra fer  
        listBox := insertar(i);  
        j := j + 1;  
    fi per  
    estat := escriure("Elements filtrats: " + string(j));  
fi funcio
```

neteja()

```
funcio neteja()  
    listBox := eliminar(inici, fi);  
    estat := escriure("Elements filtrats: "+"0");  
fi funcio
```

buscaPID()

```
funcio buscaPID()  
    pid_par := llegir();  
    mostra := executar("SELECCIONAR esdeveniments on pid := pid_par);  
    j := 0;  
    per cada i en mostra fer  
        listBox := insertar(i);  
        j := j + 1;  
    fi per  
    estat := escriure("Elements filtrats: " + string(j));  
fi funcio
```

buscaTots()

```
funcio buscaTots()  
    mostra := executar("SELECCIONAR esdeveniments");
```

```

j := 0;
per cada i en mostra fer
    listBox := insertar(i);
    j := j + 1;
fi per
estat := escriure("Elements filtrats: "+string(j))
fi funcio

```

acabar()

```

funcio acabar()
    tancaGUI()
fi funcio

```

exportaFiltrats()

```

funcio exportaFiltrats()
    per_exportar := llegir_listbox('inici', 'fi');
    fitxer_base := obrir(fitxer_bd, "afegir");
    per cada i en per_exportar
        fitxer_base := escriure(string(i));
    fi per
    fitxer_base := tanca();
    messagebox := mostrar_info(titol="Atenció", missatge="Logs exportats
correctament al fitxer de DB");
fi funcio

```

comprovaLogs()

```

funcio comprovaLogs(fitxer_logs, cursor)
    si fitxer_logs esta comprimit fer
        f := obrir_zip(fitxer_logs, 'llegir binari');
    fsi
    sino fer
        f := obrir(fitxer_logs, "llegir binari");
    fsino
    per cada i en f
        correcte := Cert;
        tipus_codif := detectar_codificacio(i);
        i := decodificar(tipus_codif);
        llista := separar_camps(llista, " ");
    fi
fi funcio

```

```

mes := llista[0];
dia := llista[1];
temps := llista[2];
temps := separar_camps(temps, ":");
hora := temps[0];
minuts := temps[1];
segons := temps[2];
correcte = comprova_data(mes, dia, hora, minuts, segons)
si correcte fer
    nom_maquina := llista[3];
    proces := llista[4];
    te_pid := buscar(proces, "[");
    si te_pid >= 0 fer
        j := 5;
        proces := separar_camps(proces, "[");
        pid := "[" + proces[1];
        proces := proces[0];
    fsi
    sino fer
        j := 4;
        pid := "" $descartar pid
    fsino
    missatge := "";
    mentre j < longitud(llista) fer
        missatge := missatge + " " + llista[j];
        j := j + 1;
    fmentre
    sql_insert := '' INSERTAR A esdeveniments (mes, dia, hora,
maquina, proces, pid, missatge) '';
    llista_mom := [mes, dia, llista[2], nom_maq, proces, pid,
missatge];
    executar(sql_insert, llista_mom);
    fsi
    sino fer
        escriu("Error de format");
    fsino
    f := tancar();
fi funcio

```


comprova_data()

```
funcio comprova_data(m, d, hora, minuto, sec):  
    correcte := Cert;  
    mesos := ['Gen', 'Ene', 'Jan', 'Feb', 'Mar', 'Abr', 'Apr', 'Mai',  
'May', 'Jun', 'Jul', 'Ago', 'Aug', 'Set', 'Sep', 'Oct', 'Nov', 'Dec',  
'Dic', 'gen', 'ene', 'jan', 'feb', 'mar', 'abr', 'apr', 'mai', 'may',  
'jun', 'jul', 'ago', 'aug', 'set', 'sep', 'oct', 'nov', 'dec', 'dic'];  
  
    si (minuto < 0 o minuto >= 60) fer  
        retorna Fals;  
    fsi  
    si (sec < 0 o sec >= 60) fer  
        retorna Fals;  
    fsi  
    si (hora < 0 o hora >= 24) fer  
        retorna Fals  
    fsi  
    si (longitud(m) != 3) fer  
        retorna Fals;  
    fsi  
    si (d <= 0 o d >= 31) fer  
        retorna Fals;  
    fsi  
    per cada i en mesos fer  
        si m == i fer  
            retorna correcte;  
        fsi  
    fper  
    retorna Fals
```

Funcions i mètodes

Descodificació

Aquesta llibreria, juntament amb el mètode `decode()`, l'hem utilitzat per a la descodificació del fitxer logs. Exemple d'ús:

«`charset.detect` Python Example». Consulta 11 març 2020.

<https://www.programcreek.com/python/example/91538/charset.detect>.

Llibreria `charset`

«`charset` — `charset` 3.0.4 documentation». Consulta 11 març de 2020.

<https://charset.readthedocs.io/en/latest/index.html>.

Definició: Detecció automàtica de la codificació dels caràcters a Python.

Funcionament: pren una seqüència d'octets en una codificació de caràcters desconeguda i intentar determinar la codificació per a que es pugui llegir el text. És com agafar un codi quan no tenim la clau de desxifrat.

Ús: `detect()` → Detecta quina codificació té la cadena de caràcters (string).

Mètode `decode()`

«Python String `decode()` Method - Tutorialspoint». Consulta 11 març 2020.

https://www.tutorialspoint.com/python/string_decode.htm.

Definició: descodifica la cadena (string) mitjançant el codec registrat per a la codificació. Per defecte descodifica segons la codificació predeterminada dels string.

Funcionament: rep per paràmetre el tipus de codificació i el mode de maneig d'errors, per defecte es 'strict', és a dir, que retorna el `UnicodeError`.

Ús: `decode()` → descodifica segons el tipus de codificació detectada.

Joc de proves

Descripció de les proves fetes, quins fitxers s'han obtingut i explicació de la seva casuística.

Bàsica



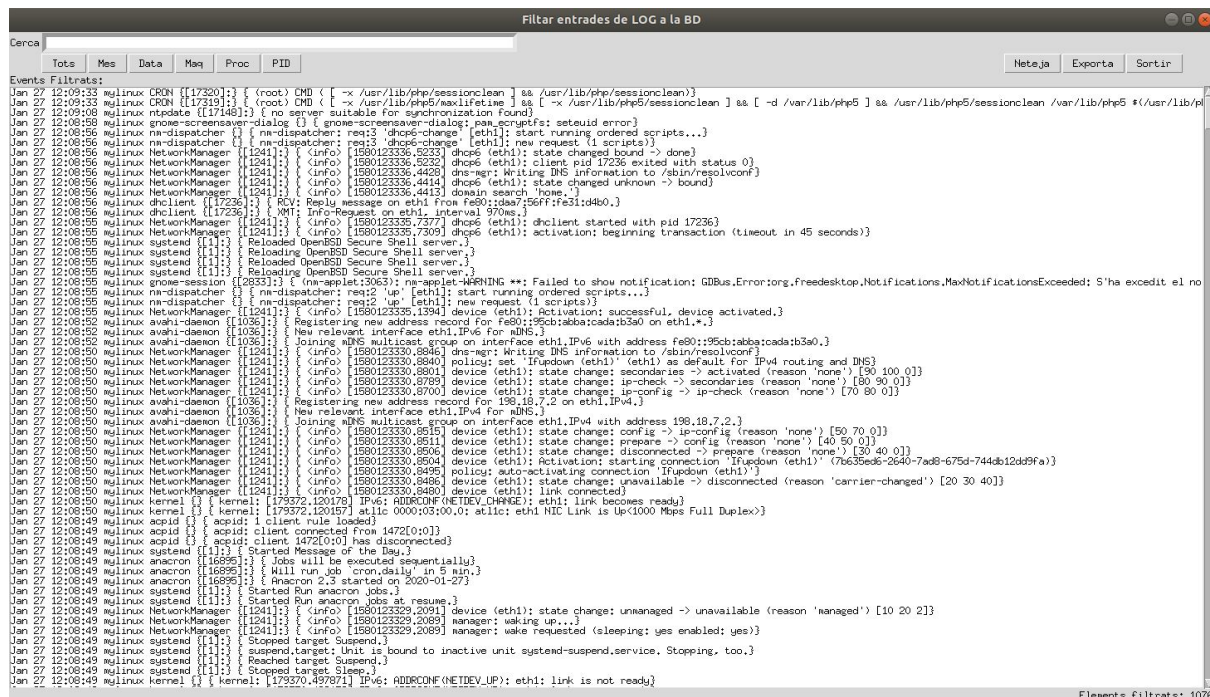
Yes Tot correcte	Ens farà escollir un fitxer de logs, si el fitxer és correcte podem utilitzar el programa
Yes Fitxer logs incorrecte	El programa es tancarà.
No Tot correcte	Escollirem el fitxer de logs i després ens demanarà la base de dades.
No Fitxers incorrectes	El programa es tancarà.



Escollim el fitxer syslog.1 per tal de fer una prova del funcionament bàsic del programa.

1. Botó “Tots”

Mostra els missatges amb el format correcte i printa per pantalla els erroris.



2. Botó “Mes”

Per a demostrar aquest cas hem fet servir els fitxers de log comprimits.

The screenshot shows the 'Filtrar entrades de LOG a la BD' window. The search bar contains 'Apr'. Below the search bar are buttons for 'Tots', 'Mes', 'Data', 'Maq', 'Proc', 'PID', 'Neteja', 'Exporta', and 'Sortir'. The 'Events Filtrats:' section displays a list of log entries. The first entry is 'Apr 23 17:24:54 netOpCenter systemd-journald [[188]:] { Journal stopped}'. The list continues with various systemd shutdown messages. At the bottom right, it says 'Elements filtrats: 9070'.

	Tots	Mes	Data	Maq	Proc	PID	Neteja	Exporta	Sortir
Events Filtrats:									
Apr 23 17:24:54	netOpCenter	systemd-journald	[[188]:]	{ Journal stopped}					
Apr 23 17:24:54	netOpCenter	systemd-shutdown	{}	{ systemd-shutdown: Sending SIGTERM t					
Apr 23 17:24:54	netOpCenter	systemd-shutdown	{}	{ systemd-shutdown: Syncing filesyste					
Apr 23 17:24:54	netOpCenter	kernel	{}	{ kernel: systemd-shutdown: 39 output lines supp					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Shutting down.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopping Monitoring of LVM2 mirrors, sna					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Starting Power-Off...}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Reached target Final Step.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Reached target Shutdown.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Create Static Device Nodes in /d					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Remount Root and Kernel File Sys					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Local File Systems (Pre).					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Swap.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Reached target Unmount All Filesystems.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Unmounted /run/user/1000.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Unmounted Temporary Directory (/tmp).}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Unmounting /run/user/1000...}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Unmounting Temporary Directory (/tmp)...}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Local File Systems.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Create Volatile Files and Direct					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Update UTMP about System Boot/Sh					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Load/Save Random Seed.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Dispatch Password Requests to Co					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Forward Password Requests to Wal					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Paths.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Removed slice User and Session Slice.}					

Elements filtrats: 9070

3. Botó Data

The screenshot shows the 'Filtrar entrades de LOG a la BD' window. The search bar contains '23'. Below the search bar are buttons for 'Tots', 'Mes', 'Data', 'Maq', 'Proc', 'PID', 'Neteja', 'Exporta', and 'Sortir'. The 'Events Filtrats:' section displays a list of log entries. The first entry is 'Apr 23 17:24:54 netOpCenter systemd {[1]:} { Unmounted Temporary Directory (/tmp).}'. The list continues with various systemd shutdown messages. At the bottom right, it says 'Elements filtrats: 2090'.

	Tots	Mes	Data	Maq	Proc	PID	Neteja	Exporta	Sortir
Events Filtrats:									
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Unmounted Temporary Directory (/tmp).}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Unmounting /run/user/1000...}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Unmounting Temporary Directory (/tmp)...}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Local File Systems.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Create Volatile Files and Direct					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Update UTMP about System Boot/Sh					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Load/Save Random Seed.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Dispatch Password Requests to Co					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Forward Password Requests to Wal					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Paths.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Removed slice User and Session Slice.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Slices.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Load Kernel Modules.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Local Encrypted Volumes.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Update UTMP about System Boot/S					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Apply Kernel Variables.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopping Load/Save Random Seed...}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target System Initialization.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Closed D-Bus System Message Bus Socket.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Sockets.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped target Basic System.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Started Generate shutdown-ramfs.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Login Service.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Network Service.}					
Apr 23 17:24:54	netOpCenter	mkinitcpio	[[528]:]	{ ==> Build complete.}					
Apr 23 17:24:54	netOpCenter	systemd	{[1]:}	{ Stopped Open vSwitch Database Server.}					

Elements filtrats: 2090

4. Botó Maq

Filtar entrades de LOG a la BD

Cerca

Tots Mes Data Maq Proc PID Neteja Exporta Sortir

Events Filtrats:

Jan 27 12:08:55	mylinux	systemd	[1]::	Reloaded OpenBSD Secure Shell server.}
Jan 27 12:08:55	mylinux	systemd	[1]::	Reloading OpenBSD Secure Shell server.}
Jan 27 12:08:55	mylinux	systemd	[1]::	Reloaded OpenBSD Secure Shell server.}
Jan 27 12:08:55	mylinux	systemd	[1]::	Reloading OpenBSD Secure Shell server.}
Jan 27 12:08:49	mylinux	systemd	[1]::	Started Message of the Day.}
Jan 27 12:08:49	mylinux	systemd	[1]::	Started Run anacron jobs.}
Jan 27 12:08:49	mylinux	systemd	[1]::	Started Run anacron jobs at resume.}
Jan 27 12:08:49	mylinux	systemd	[1]::	Stopped target Suspend.}
Jan 27 12:08:49	mylinux	systemd	[1]::	suspend.target: Unit is bound to inactive unit systemd-s
Jan 27 12:08:49	mylinux	systemd	[1]::	Reached target Suspend.}
Jan 27 12:08:49	mylinux	systemd	[1]::	Stopped target Sleep.}
Jan 27 12:08:49	mylinux	systemd	[1]::	sleep.target: Unit not needed anymore. Stopping.}
Jan 27 12:08:49	mylinux	systemd	[1]::	Started Suspend.}
Jan 27 12:08:49	mylinux	systemd	[1]::	Starting Daily apt download activities...}
Jan 27 12:08:49	mylinux	systemd	[1]::	Starting Message of the Day...}
Jan 27 12:08:49	mylinux	systemd	[1]::	Time has been changed}
Jan 27 12:08:49	mylinux	systemd	[8849]::	Time has been changed}
Jan 27 12:08:49	mylinux	systemd	[2581]::	Time has been changed}
Jan 26 21:29:13	mylinux	systemd	[1]::	Starting Suspend...}
Jan 26 21:29:13	mylinux	systemd	[1]::	Reached target Sleep.}
Jan 26 21:29:13	mylinux	systemd	[1]::	Started Network Manager Script Dispatcher Service.}
Jan 26 21:29:13	mylinux	systemd	[1]::	Starting Network Manager Script Dispatcher Service...}
Jan 26 21:27:55	mylinux	systemd	[1]::	Started Hostname Service.}
Jan 26 21:27:55	mylinux	systemd	[1]::	Starting Hostname Service...}
Jan 26 21:22:54	mylinux	systemd	[1]::	Started Session 458 of user jomateix.}
Jan 26 21:14:23	mylinux	systemd	[1]::	Started Session 455 of user jomateix.}
Jan 26 21:12:25	mylinux	systemd	[1]::	Started Session 454 of user jomateix.}

Elements filtrats: 0

5. Botó Proc

Filtar entrades de LOG a la BD

Cerca

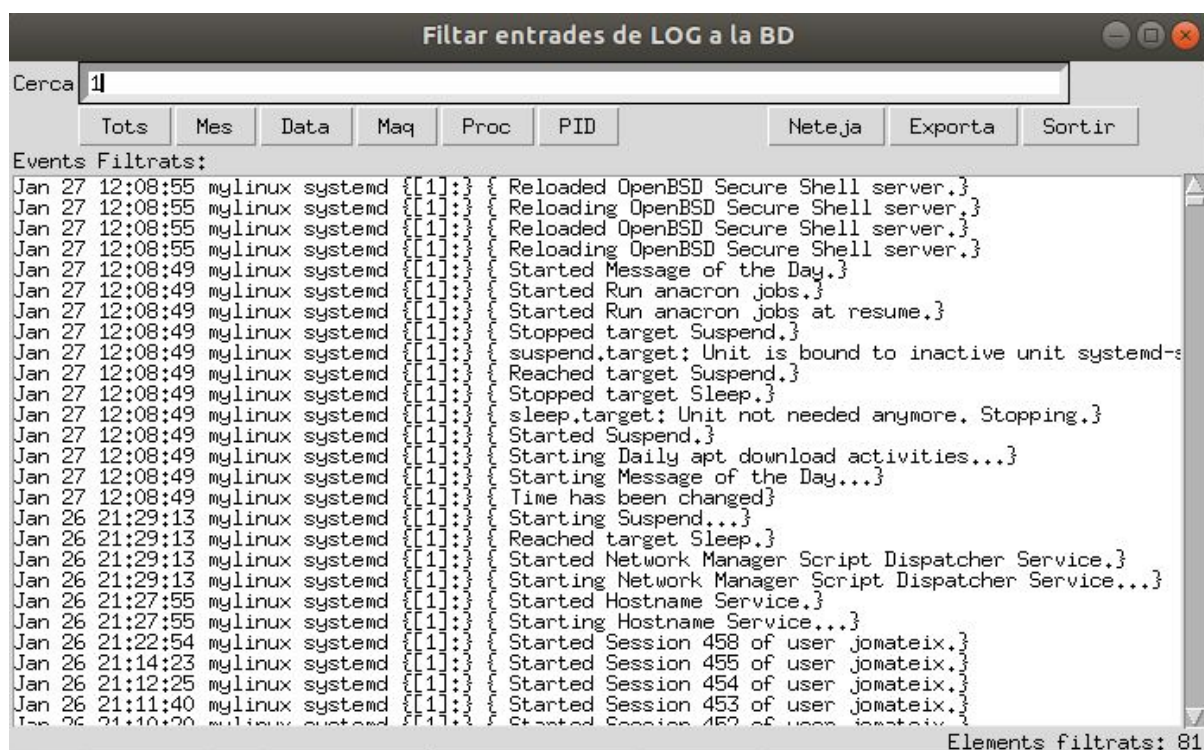
Tots Mes Data Maq Proc PID Neteja Exporta Sortir

Events Filtrats:

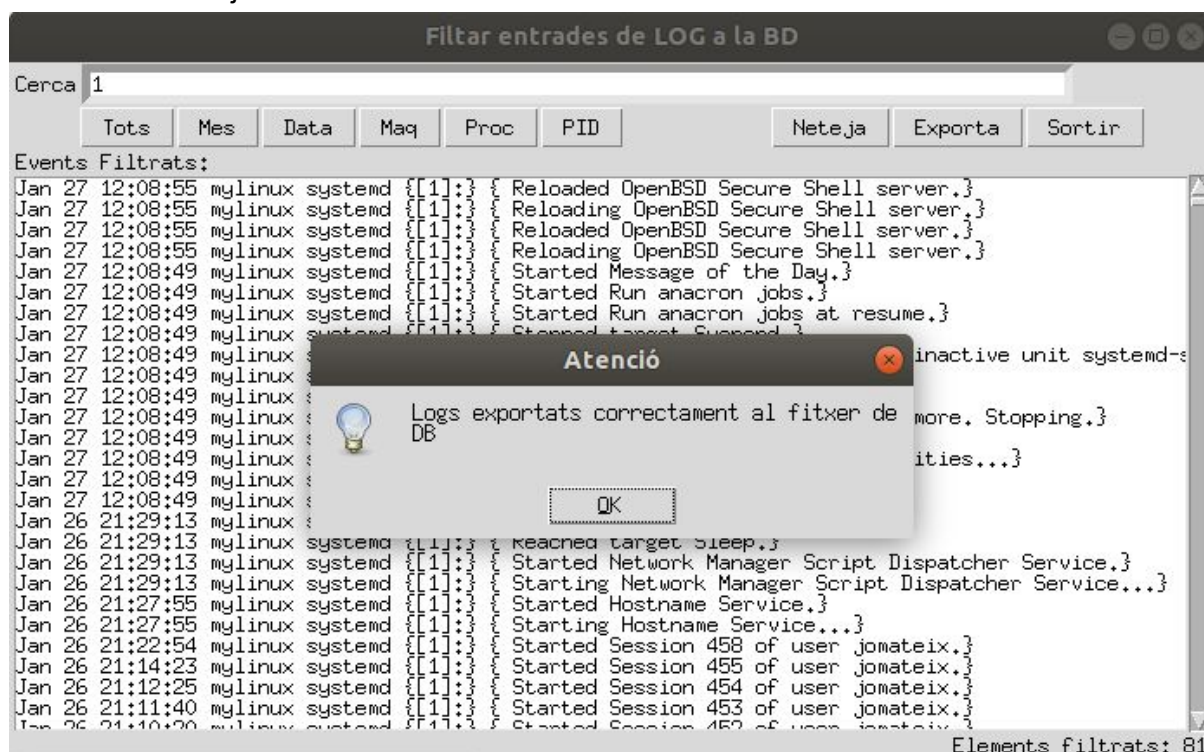
Jan 27 12:08:50	mylinux	kernel	[179372.120178]	IPv6: ADDRCONF (NETDEV_CHANGE): eth1:
Jan 27 12:08:50	mylinux	kernel	[179372.120157]	atl1c 0000:03:00.0: atl1c: eth1 NIC l
Jan 27 12:08:49	mylinux	kernel	[179370.497871]	IPv6: ADDRCONF (NETDEV_UP): eth1: link
Jan 27 12:08:49	mylinux	kernel	[179370.482139]	IPv6: ADDRCONF (NETDEV_UP): eth1: link
Jan 27 12:08:49	mylinux	kernel	[179370.295491]	Restarting tasks ... done.}
Jan 27 12:08:49	mylinux	kernel	[179370.295490]	PM: Finishing wakeup.}
Jan 27 12:08:49	mylinux	kernel	[179370.290153]	PM: resume of devices complete after
Jan 27 12:08:49	mylinux	kernel	[179370.148036]	usb 4-2.4: reset full-speed USB device
Jan 27 12:08:49	mylinux	kernel	[179370.004136]	ata2.00: configured for UDMA/100}
Jan 27 12:08:49	mylinux	kernel	[179369.988143]	ata2.00: ACPI cmd ef/03:0c:00:00:00:a
Jan 27 12:08:49	mylinux	kernel	[179369.988139]	ata2.00: ACPI cmd ef/03:45:00:00:00:a
Jan 27 12:08:49	mylinux	kernel	[179369.988136]	ata2.00: ACPI cmd ef/03:45:00:00:00:a
Jan 27 12:08:49	mylinux	kernel	[179369.980249]	ata2.01: NODEV after polling detectio
Jan 27 12:08:49	mylinux	kernel	[179369.696058]	usb 4-2: reset full-speed USB device
Jan 27 12:08:49	mylinux	kernel	[179369.592309]	ata1.01: configured for UDMA/133}
Jan 27 12:08:49	mylinux	kernel	[179369.577289]	ata1.00: configured for UDMA/133}
Jan 27 12:08:49	mylinux	kernel	[179369.576860]	ata1.00: ACPI cmd ef/03:0c:00:00:00:a
Jan 27 12:08:49	mylinux	kernel	[179369.576858]	ata1.00: ACPI cmd ef/03:45:00:00:00:a
Jan 27 12:08:49	mylinux	kernel	[179369.576855]	ata1.00: ACPI cmd ef/03:45:00:00:00:a
Jan 27 12:08:49	mylinux	kernel	[179369.544273]	ata1.01: ACPI cmd ef/03:0c:00:00:00:k
Jan 27 12:08:49	mylinux	kernel	[179369.544271]	ata1.01: ACPI cmd ef/03:45:00:00:00:k
Jan 27 12:08:49	mylinux	kernel	[179369.544268]	ata1.01: ACPI cmd ef/03:45:00:00:00:k
Jan 27 12:08:49	mylinux	kernel	[179369.379845]	sd 0:0:1:0: [sdb] Starting disk}
Jan 27 12:08:49	mylinux	kernel	[179369.379807]	sd 0:0:0:0: [sda] Starting disk}
Jan 27 12:08:49	mylinux	kernel	[179369.379034]	parport_pc 00:04: activated}
Jan 27 12:08:49	mylinux	kernel	[179369.378638]	serial 00:03: activated}
Jan 27 12:08:49	mylinux	kernel	[179369.378609]	serial 00:02: activated}

Elements filtrats: 333

6. Botó PID



7. Botó Neteja



8. Botó Exporta

Filtrar entrades de LOG a la BD

Cerca 1

Tots Mes Data Maq Proc PID Neteja Exporta Sortir

Events Filtrats:

Jan 27 12:08:55	mylinux	systemd	{[1]:}	{	Reloaded OpenBSD Secure Shell server.}
Jan 27 12:08:55	mylinux	systemd	{[1]:}	{	Reloading OpenBSD Secure Shell server.}
Jan 27 12:08:55	mylinux	systemd	{[1]:}	{	Reloaded OpenBSD Secure Shell server.}
Jan 27 12:08:55	mylinux	systemd	{[1]:}	{	Reloading OpenBSD Secure Shell server.}
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	Started Message of the Day.}
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	Started Run anacron jobs.}
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	Started Run anacron jobs at resume.}
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	Stopped target Suspend.}
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	inactive unit systemd-s
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	more. Stopping.}
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	ities...}
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	
Jan 27 12:08:49	mylinux	systemd	{[1]:}	{	
Jan 26 21:29:13	mylinux	systemd	{[1]:}	{	Reached target Sleep.}
Jan 26 21:29:13	mylinux	systemd	{[1]:}	{	Started Network Manager Script Dispatcher Service.}
Jan 26 21:29:13	mylinux	systemd	{[1]:}	{	Starting Network Manager Script Dispatcher Service...}
Jan 26 21:27:55	mylinux	systemd	{[1]:}	{	Started Hostname Service.}
Jan 26 21:27:55	mylinux	systemd	{[1]:}	{	Starting Hostname Service...}
Jan 26 21:22:54	mylinux	systemd	{[1]:}	{	Started Session 458 of user jomateix.}
Jan 26 21:14:23	mylinux	systemd	{[1]:}	{	Started Session 455 of user jomateix.}
Jan 26 21:12:25	mylinux	systemd	{[1]:}	{	Started Session 454 of user jomateix.}
Jan 26 21:11:40	mylinux	systemd	{[1]:}	{	Started Session 453 of user jomateix.}
Jan 26 21:10:20	mylinux	systemd	{[1]:}	{	Started Session 452 of user jomateix.}

Atenció

Logs exportats correctament al fitxer de DB

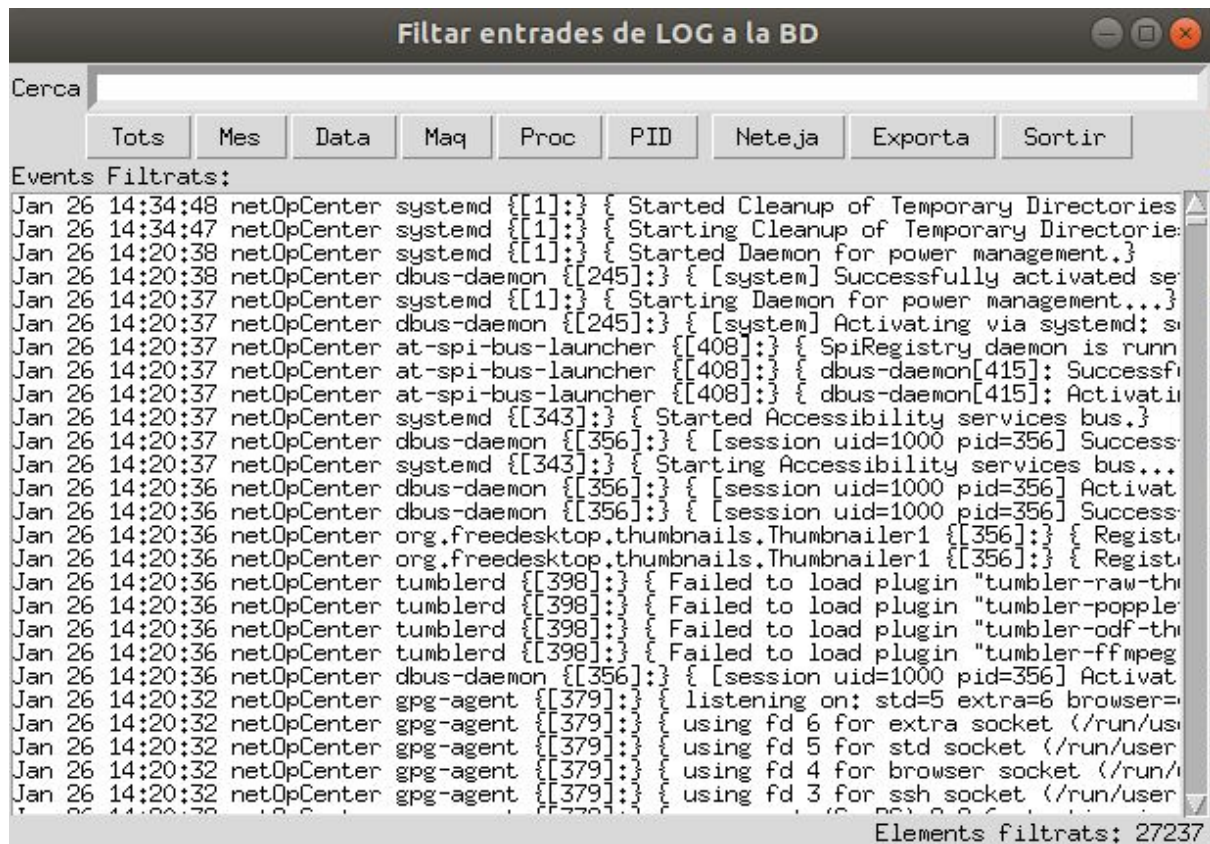
OK

Elements filtrats: 81

Documents FSO_19-20 P1 RESULT

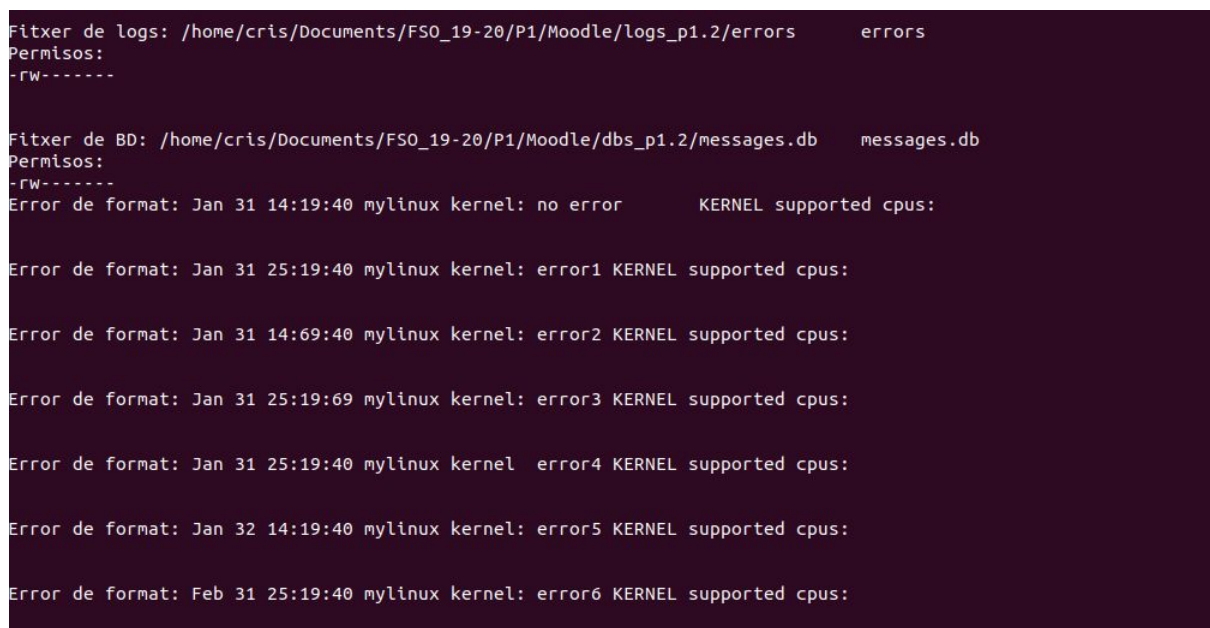
logs2db
150320.db

Comprimida



Triga més en carregar però el funcionament acaba sent el mateix.

Errònia



En el cas de provar amb el fitxer de logs amb errors obtenim aquesta sortida.