

Exercicis SSMTP

Escribe un script que cada vez que root se conecte remotamente por consola, el sistema envíe un email a un determinado usuario, indicándole:

- Hora de inicio de la sesión
- Punto (consola, ip) desde el que se ha realizado la conexión

```
#
# Some more alias to avoid making mistakes
# alias rm='rm -i'
# alias cp='cp -i'
# alias mv='mv -i'

/home/daniel/alertaRoot.sh
```

.bashrc per usuari Root

```
#!/bin/bash
cat /dev/null > /home/daniel/alertaRoot.txt
echo -e "To:daniel.hernandez@gracia.lasalle.cat" > /home/daniel/alertaRoot.txt
echo -e "From:daniel.hernandez@gracia.lasalle.cat" >> /home/daniel/alertaRoot.txt
echo -e "Subject:ALERTA CONEXIO ROOT\n" >> /home/daniel/alertaRoot.txt
hora=$(date | awk '{print $4}')
ip=$(ip a | grep "inet " | grep -v "127.0.0.1" | awk '{print $2}')
tty=$(who am i | awk '{print $2}')
echo "Root conectat a les $hora a traves de la IP: $ip amb la tty: $tty" >> /home/daniel/alertaRoot.txt
ssmtp daniel.hernandez@gracia.lasalle.cat < /home/daniel/alertaRoot.txt
```

Script que executa .bashrc al conectar-se Root



Missatge rebut a l'hora de conectar-se root.

Script que evalúe la ocupación de los diferentes puntos de montaje de nuestro sistema.

- Nos enviará un email en el momento que la ocupación supere un determinado % de ocupación.
- El email nos dará información del disco en cuestión, así como la ocupación del resto de los discos.

```
#!/bin/bash

llista_ocupa=$(df -h | sed 1d | awk '{print $5}' | tr -d '%')
count=0
sobre="false"

cat /dev/null > ocupaDiscos.txt
echo -e "To:daniel.hernandez@gracia.lasalle.cat" >> ocupaDiscos.txt
echo -e "From:daniel.hernandez@gracia.lasalle.cat" >> ocupaDiscos.txt
echo -e "Subject:Alerta Disc superat" >> ocupaDiscos.txt
echo "" >> ocupaDiscos.txt

for pcnt in $llista_ocupa
do
    ((count++))
    if [[ $pcnt -gt 5 ]]
    then
        sobre="true"
        nomdisk=$(df -h | sed 1d | awk -v count=$count 'NR==count {print $1}')
        percentdisk=$(df -h | sed 1d | awk -v count=$count 'NR==count {print $5}')
        echo "[+] El disc $nomdisk esta per sobre del 5%, ocupacio actual: ${percentdisk}" >
    > ocupaDiscos.txt
        echo "" >> ocupaDiscos.txt
    fi
done
echo "La resta de discos es troben a:" >> ocupaDiscos.txt
echo "" >> ocupaDiscos.txt
echo "Nom disc" ----- "% ocupacio" >> ocupaDiscos.txt
df -h | sed 1d | awk '{print $1, "-----", $5}' >> ocupaDiscos.txt

if [[ $sobre == "true" ]]
then
    ssmtp daniel.hernandez@gracia.lasalle.cat < ocupaDiscos.txt
fi
```

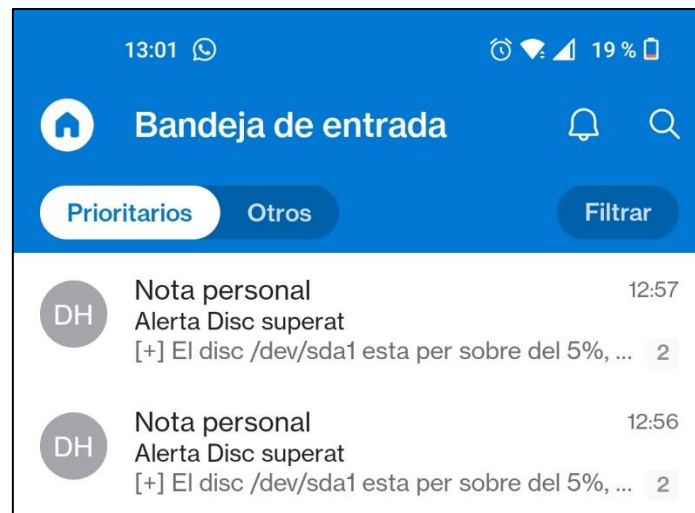
Script que controlar ocupación de cada disc, crea i envía mail si sobrepasa un llindar

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

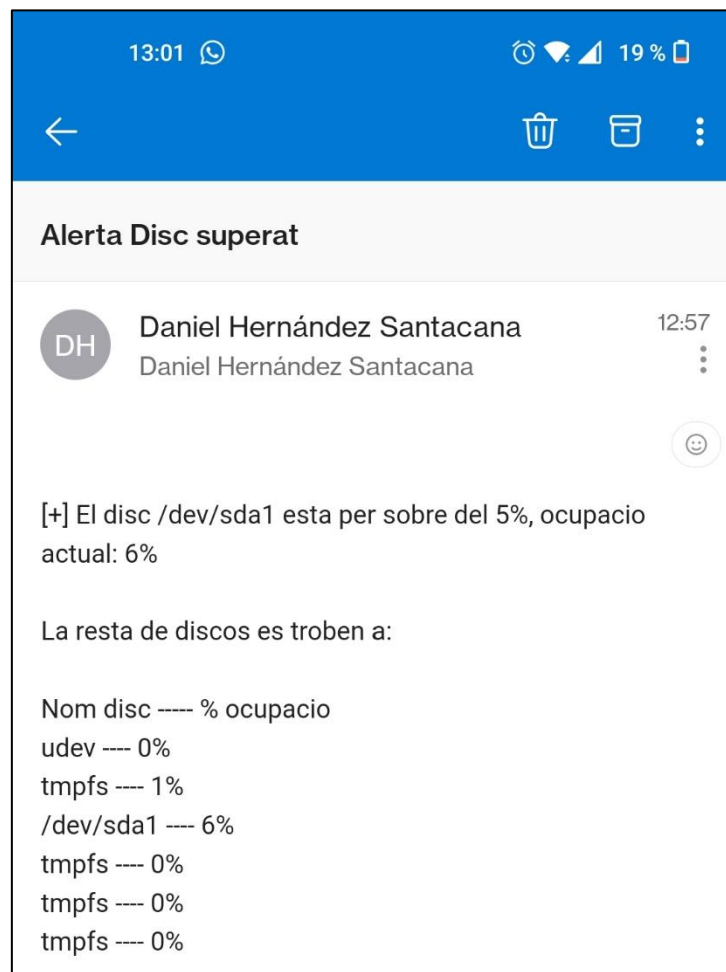
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-
)
* * * * * daniel /home/daniel/scripts/ssmtp/checkHDD.sh
#
```

Creació de la tasca crontab a través de /etc/crontab (amb crontab -e no anava)



Spam de disc per sobre a través de crontab



Cada minut comprova la ocupació i m'actualitza amb un correu
 Observem la informació del disc afectat i la ocupació de tots els discos

(podríem treure els tmpfs amb un grep, inclús si nomes volguéssim altres discos extra i no el
 afectat també grapejar el nom dels anteriors fora amb una llista)

Script que cada x temps analitzi els recursos de xarxa i miri si ha caigut algun element de xarxa.

- Els elements de xarxa han de estar prèviament definits per l'usuari.
- Aquests es poden avaluar mitjançant connectivitat per ping (cas de switches, routers, ...), o mitjançant l'avaluació de la disponibilitat del servei (cas de servidors web, servidor ssh, ...)

```
#!/bin/bash
lista_ips=$(prips 10.0.2.0/24)
cat /dev/null > ip_conectadas.txt

for ip in $lista_ips
do
    timeout 1 ping -c 1 $ip > /dev/null 2>&1 && echo $ip >> ip_conectadas.txt &
done

if [ -f ip_backup.txt ]
then
    ip_dif=$(diff ip_conectadas.txt ip_backup.txt)
fi

cat /dev/null > msg_xarxa.txt
echo -e "To:daniel.hernandez@gracia.lasalle.cat" >> msg_xarxa.txt
echo -e "From:daniel.hernandez@gracia.lasalle.cat" >> msg_xarxa.txt
echo -e "Subject:Alerta de la xarxa" >> msg_xarxa.txt
echo "" >> msg_xarxa.txt

simbol=$(echo $ip_dif | awk '{print $2}')
ip_ref=$(echo $ip_dif | awk '{print $3}')
contingut=0
if [[ $simbol == ">" ]]
then
    echo "La IP $ip_ref s'ha caigut" >> msg_xarxa.txt
    contingut=1
elif [[ $simbol == "<" ]]
then
    echo "La IP $ip_ref s'ha connectat" >> msg_xarxa.txt
    contingut=1
fi

cp ip_conectadas.txt ip_backup.txt

if [[ $contingut -eq 1 ]]
then
    smtp daniel.hernandez@gracia.lasalle.cat < msg_xarxa.txt
fi
```

Script on comprovo els dispositius connectats a la xarxa, i si algun es connecta o cau cada minut m'avisarà enviant un correu

```

PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,w
# | | | | |
# * * * * * user-name command to be executed
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts
)
* * * * * daniel  /home/daniel/scanPing.sh
#

```

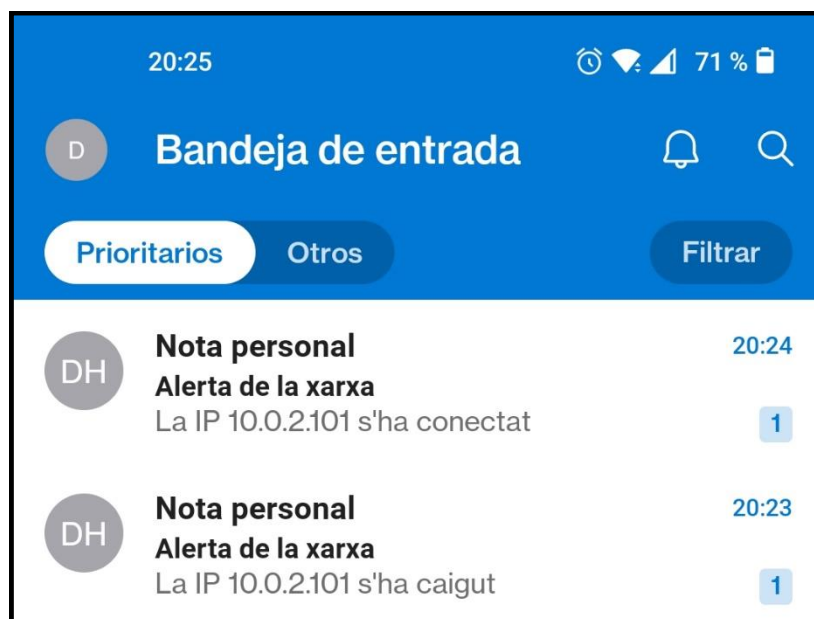
Creació del crontab

```

daniel@hackeame:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    link/ether 00:0c:29:05:d0:fb brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.0.2.101/24 metric 100 brd 10.0.2.255 scope global dynamic
        valid_lft 1219sec preferred_lft 1219sec
    inet6 fe80::20c:29ff:fe05:d0fb/64 scope link
        valid_lft forever preferred_lft forever

```

Connecto una nova maquina i la desconnecto passat un minut



Rebem missatge d'avis