

# Scripts departamento Ingenieria

## Crontab

```
GNU nano 6.2 /tmp/crontab.m0p2Km/crontab *
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command

#Transferencia de datos de cada sesion de ingenieria a simulacion
30 14 * * 5-7 sh /home/cliente/ingenieria/transferencia_datos.sh

#Monitorizacion de red
59 13 * * 5-7 sh /home/cliente/ingenieria/monitorizacion_red.sh
#Descarga archivos
0 14 * * 5-7 sh /home/cliente/ingenieria/descarga.sh
#Iptable enable 8:00 viernes a domingo
0 8 * * 5-7 sh /home/cliente/ingenieria/iptables_enable.sh

#Iptable disable 12:00 viernes a domingo
0 12 * * 5-7 sh /home/cliente/ingenieria/iptables_disable.sh

#Iptable enable 13:00 viernes a domingo
0 13 * * 5-7 sh /home/cliente/ingenieria/iptables_enable.sh

#Crear copia seguridad
0 16 * * 5-7 sh /home/cliente/ingenieria/copia_seguridad.sh

#Shutdown equipos automatico al finalizar la jornada laboral
30 17 * * 5-7 sh /home/cliente/ingenieria/shutdown_equipos.sh

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

#Transferencia de datos de cada sesion de ingenieria a simulacion

30 14 \* \* 5-7 sh /home/cliente/ingenieria/transferencia\_datos.sh

#Monitorizacion de red

59 13 \* \* 5-7 sh /home/cliente/ingenieria/monitorizacion\_red.sh

#Descarga archivos

0 14 \* \* 5-7 sh /home/cliente/ingenieria/descarga.sh

#Iptable enable 8:00 viernes a domingo

0 8 \* \* 5-7 sh /home/cliente/ingenieria/iptables\_enable.sh

#Iptable disable 12:00 viernes a domingo

0 12 \* \* 5-7 sh /home/cliente/ingenieria/iptables\_disable.sh

#Iptable enable 13:00 viernes a domingo

0 13 \* \* 5-7 sh /home/cliente/ingenieria/iptables\_enable.sh

#Crear copia seguridad

0 16 \* \* 5-7 sh /home/cliente/ingenieria/copia\_seguridad.sh

#Shutdown equipos automatico al finalizar la jornada laboral

30 17 \* \* 5-7 sh /home/cliente/ingenieria/shutdown\_equipos.sh

## Script de transferencia de datos

```
GNU nano 6.2          transferencia_datos.sh          S
#!/bin/sh

#Abrir puertos
sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP
echo "Puertos abiertos"

#Envio de la informacion
scp /home/cliente/ingenieria/datos/sesion_entrenamiento.txt server@192.168.18.61:/home/server/simulacion/datos/

#Cerrar puertos
sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP
echo "Puertos cerrados"

[ Soft wrapping of overlong lines enabled ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

#!/bin/sh

#Abrir puertos (no es necesario este paso)

sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP

echo "Puertos abiertos"

#Envio de la informacion

scp /home/cliente/ingenieria/datos/sesion\_entrenamiento.txt server@192.168.18.61:  
/home/server/simulacion/datos/

#Cerrar puertos (no es necesario este paso)

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP

echo "Puertos cerrados"

## Script monitorización de red

```
GNU nano 6.2 monitorizacion_red.sh
#!/bin/sh

#Nombre del archivo de salida
output_file="/home/cliente/ingenieria/datos/monitorizacion.txt"

#Funcion para monitorizar la red con iftop
monitorizar_red(){
echo "Monitorizando red"
sudo iftop -t -s 2 -n > "$output_file"
}

monitorizar_red

#Descargar el archivo
echo "Ejecutando el script de descarga"

./descarga.sh

#Monitorizar la red despues de la descarga
echo "Monitorizando la red despues de la descarga"
monitorizar_red
```

[ Read 29 lines ]

Help Write Out Where Is Cut Execute Location M-U Undo  
Exit Read File Replace Paste Justify Go To Line M-E Redo

#!/bin/sh

#Nombre del archivo de salida

output\_file="/home/cliente/ingenieria/datos/monitorizacion.txt"

#Funcion para monitorizar la red con iftop

monitorizar\_red () {

echo "Monitorizando red"

sudo iftop -t -s 2 -n > "\$output\_file"

monitorizar\_red

#Descargar el archivo

echo "Ejecutando el script de descarga"

./descarga.sh

#Monitorizar la red despues de la descarga

echo "Monitorizando la red despues de la descarga"

monitorizar\_red

## Script descarga archivos

```
GNU nano 6.2                                descarga.sh
#!/bin/sh

#Abrimos los puertos
sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP
echo "Puertos abiertos"

#URL del archivo
url="https://cdn-6.motorsport.com/images/mg1/6AEomeD6/s800/fernando-alonso-aston-martin-r-1.jpg"

#Ruta de destino
ruta_destino="/home/cliente/ingenieria/informacion_pista/"

#Navega la carpeta destino
cd "$ruta_destino"

#Descarga
sudo wget "$url"

#Cierro puertos
sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP
```

[ Read 28 lines ]

Help Write Out Where Is Cut Execute Location M-U Undo  
Exit Read File Replace Paste Justify Go To Line M-E Redo

#!/bin/sh

#Abrimos los puertos

sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP

echo "Puertos abiertos"

#URL del archivo

url="https://cdn-6.motorsport.com/images/mg1/6AEomeD6/s800/fernando-alonso-aston-martin-r-1.jpg"

#Ruta de destino

ruta\_destino="/home/cliente/ingenieria/informacion\_pista/"

#Navega la carpeta destino

"\$ruta\_destino"

#Descarga

sudo wget "\$url"

#Cierro puertos

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP

## Script iptable\_enable

```
GNU nano 6.2                                iptables_enable.sh
#!/bin/sh

#Abrimos los puertos

sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP
```

#!/bin/sh

#Abrimos los puertos

sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP

echo "Puertos abiertos"

## Script iptable\_disable

```
GNU nano 6.2                                iptables_disable.sh
#!/bin/sh

#Cerrar conexion a internet

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP
```

#!/bin/sh

#Cerramos los puertos

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP

## Script copia de seguridad

```
GNU nano 6.2                                copia_seguridad.sh
#!/bin/sh

#Cerrar la conexion a internet

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP
echo "Acceso a internet restringido"

#Realizamos la copia de seguridad
cd /home/cliente/ingenieria
tar -czvf copia_seguridad.tar.gz .
echo "Copia seguridad hecha"

#Abrimos la conexion a internet de nuevo
sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP

echo "Acceso a internet permitido"
```

#!/bin/sh

#Cerrar la conexion a internet

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP

echo "Acceso a internet restringido"

#Realizamos la copia de seguridad

cd /home/cliente/ingenieria

tar -czvf copia\_seguridad.tar.gz.

echo "Copia seguridad hecha"

#Abrimos la conexion a internet de nuevo

sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP

echo "Acceso a internet permitido"

## Script shutdown equipos

```
GNU nano 6.2 shutdown_equipos.sh
#!/bin/sh

echo "El equipo se apagará en 5 segundos"

sleep 5

shutdown -h now
```

#!/bin/sh

echo "El equipo se apagará en 5 segundos"

sleep 5

shutdown -h now

## Scripts Simulación

### Crontab

```
GNU nano 6.2 /tmp/crontab.LjibK7/crontab S
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
#Crear copia de seguridad
0 4 * * 5-7 sh /home/server/simulacion/copia_seguridad.sh

#Enviar datos con los resultados obtenidos
0 8 * * 5-7 sh /home/server/simulacion/transferencia_datos.sh

[ Soft wrapping of overlong lines enabled ]
Help Write Out Where Is Cut Execute Location M-U Undo
Exit Read File Replace Paste Justify Go To Line M-E Redo
```

#Crear copia de seguridad

0 4 \* \* 5-7 sh /home/server/simulacion/copia\_seguridad.sh

#Enviar datos con los resultados obtenidos

0 8 \* \* 5-7 sh /home/server/simulacion/transferencia\_datos.sh

## Script copia\_seguridad

```
GNU nano 6.2                                copia_seguridad.sh
#!/bin/sh

#Cerrar la conexion a internet

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP
echo "Acceso a internet restringido"

#Realizamos la copia de seguridad
cd /home/server/simulacion
tar -czvf copia_seguridad.tar.gz .
echo "Copia seguridad hecha"

#Abrimos los puertos
sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP
sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP

echo "Acceso a internet permitido"
```

#!/bin/sh

#Cerrar la conexion a internet

sudo iptables -A OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -A OUTPUT -p tcp --dport 443 -j DROP

echo "Acceso a internet restringido"

#Realizamos la copia de seguridad

cd /home/server/simulacion

tar -czvf copia\_seguridad.tar.gz .

echo "Copia seguridad hecha"

#Abrimos la conexion a internet de nuevo

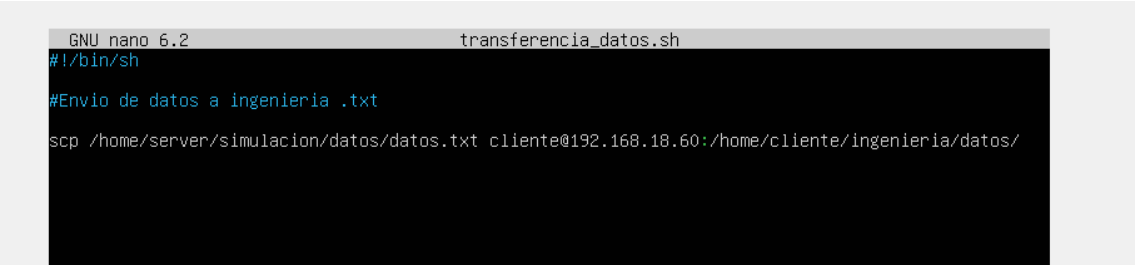
sudo iptables -D OUTPUT -p tcp --dport 80 -j DROP

sudo iptables -D OUTPUT -p tcp --dport 443 -j DROP

echo "Acceso a internet permitido"



## Script transferencia\_datos



```
GNU nano 6.2 transferencia_datos.sh
#!/bin/sh

#Envio de datos a ingenieria .txt

scp /home/server/simulacion/datos/datos.txt cliente@192.168.18.60:/home/cliente/ingenieria/datos/
```

#!/bin/sh

#Envio de datos a ingenieria .txt

scp /home/server/simulacion/datos/datos.txt  
cliente@192.168.18.60:/home/cliente/ingenieria/datos/

A tener en cuenta varias cosas:

Las rutas, los nombres de usuario y las ips serán diferentes en cada caso, en el mío estas son las necesarias.

Si se desea adelantar la hora o atrasar con los comandos pertinentes, no se podrá ejecutar mas de un crontab a la vez, creará un conflicto, si se ejecuta el programa las 24h del dia, este conflicto desaparecerá.