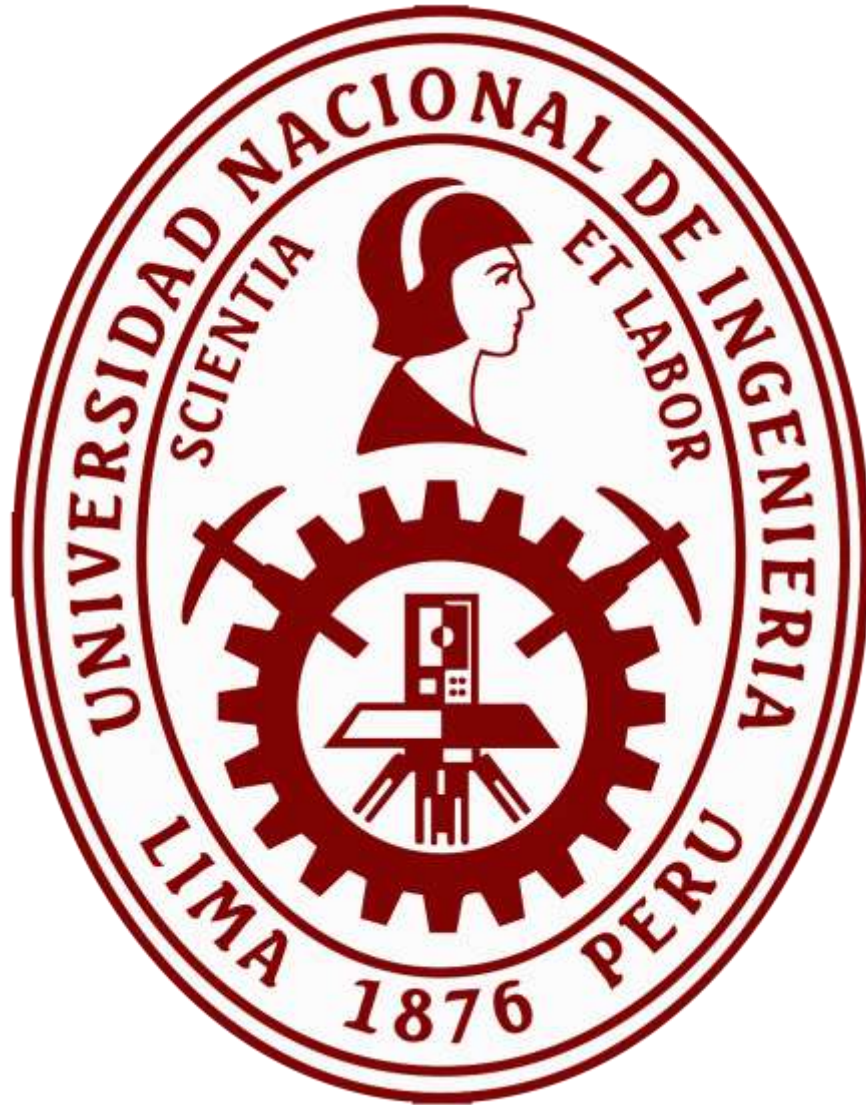


## Laboratorio 04: Monitorización del sistema



Asignatura: Administración de Redes

Nombre: Carlos Alberto Espinoza Mansilla

## **INDICE**

ACTIVIDAD 3 .....	3
ACTIVIDAD 4 .....	4
LINK:videotutorial.....	6

### ACTIVIDAD 3

1. Con el comando `crontab -e` seteamos lo que se nos pide:

- ✓ 15 minutos después de la medianoche todos los sábados.
- ✓ El primer día de cada mes a las 3:30 AM.

el formato es de la forma: min hora día(del mes) mes día(de semana) usuario archivo



```
admin@localhost:~  
File Edit View Search Terminal Help  
15 0 * * 6 admin /home/admin/progreso.sh  
30 15 1 * * admin /home/admin/progreso.sh
```

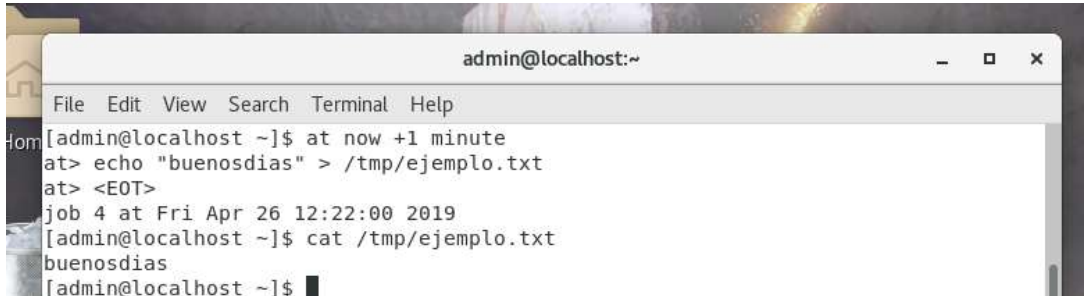
de nuevo con `crontab -e` aplicamos para `(date >> /tmp/salida)` cada 5 minutos



```
admin@localhost:~  
File Edit View Search Terminal Help  
15 0 * * 6 admin /home/admin/progreso.sh  
30 15 1 * * admin /home/admin/progreso.sh  
5 * * * * admin date >> /tmp/salida
```

2. usamos `at` para mandar un mensaje

`echo "buenos dias" > /tmp/ejemplo.txt`



```
admin@localhost:~  
File Edit View Search Terminal Help  
[admin@localhost ~]$ at now +1 minute  
at> echo "buenosdias" > /tmp/ejemplo.txt  
at> <EOT>  
job 4 at Fri Apr 26 12:22:00 2019  
[admin@localhost ~]$ cat /tmp/ejemplo.txt  
buenosdias  
[admin@localhost ~]$
```

## ACTIVIDAD 4

1. Comprobar que el paquete rsyslog está instalado y que está en ejecución.

```
Package rsyslog-8.24.0-34.el7.x86_64 already installed and latest version
Nothing to do
[root@localhost admin]#
```

2. El archivo de configuración es /etc/rsyslog.conf. Estudiar la sección rules, cada regla hace referencia <servicio>.<severidad>. Los servicios son authpriv, cron, kern, mail, news, user, y uucp; y los niveles de severidad, de menor a mayor son: debug, info, notice, warn, err, crit, alert, emerg.

Este archivo de configuración lo que hace es indicar bajo qué circunstancias y en qué carpetas se van a grabar los logs al ejecutar alguna acción.

```
### RULES ###

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                          /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none      /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                     /var/log/secure

# Log all the mail messages in one place.
mail.*                                          -/var/log/maillog

# Log cron stuff
cron.*                                         /var/log/cron

# Everybody gets emergency messages
*.emerg                                        :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                /var/log/spooler

# Save boot messages also to boot.log
local7.*                                       /var/log/boot.log

# ### begin forwarding rule ###
# The statement between the begin and define is a TRIGGER Forwarding
```

3. Estudiar los archivos de log en /var/log, ejemplo boot.log, syslog. y auth.log.

De acuerdo a lo observado dentro de boot.log, syslog y auth.log en estos archivos se guardan todas las acciones que acaban en error. Por ejemplo, en mi archivo /var/log/boot.log-20190330 se guarda un booteo del sistema fallido.

```
File Edit View Search Terminal Help
Starting Network Manager Wait Online...
Starting Hostname Service...
[ OK ] Started Hostname Service.
Starting Network Manager Script Dispatcher Service...
[ OK ] Started Network Manager Script Dispatcher Service.
[ OK ] Started Network Manager Wait Online.
Starting LSB: Bring up/down networking...
[ OK ] Started LSB: Bring up/down networking.
[ OK ] Reached target Network.
[ OK ] Reached target Network is Online.
Starting Notify NFS peers of a restart...
[ OK ] Started CUPS Printing Service.
Starting Postfix Mail Transport Agent...
Starting Logout off all iSCSI sessions on shutdown...
Starting Dynamic System Tuning Daemon...
Starting OpenSSH server daemon...
Starting System Logging Service...
[ OK ] Started Notify NFS peers of a restart.
[ OK ] Started Logout off all iSCSI sessions on shutdown.
[ OK ] Reached target Remote File Systems (Pre).
[ OK ] Reached target Remote File Systems.
Starting Permit User Sessions...
Starting Crash recovery kernel arming...
Starting Virtualization daemon...
Starting Availability of block devices...
[ OK ] Started System Logging Service.
[ OK ] Started Availability of block devices.
[ OK ] Started Permit User Sessions.
[ OK ] Started Job spooling tools.
[ OK ] Started Command Scheduler.
Starting GNOME Display Manager...
[ OK ] Started OpenSSH server daemon.
[ FAILED ] Failed to start Crash recovery kernel arming.
See 'systemctl status kdump.service' for details.
[root@localhost admin]# cat /var/log/boot.log-20190330
```

4. Los archivos de log pueden crecer demasiado lo que dificulta su manejo. Por defecto la utilidad logrotate rota los logs cada semana. Estudiar los contenidos de /etc/logrotate.conf y los archivos de configuración específicos de cada servicio en /etc/logrotate.d.

El archivo /etc/logrotate.conf especifica que serán 4 semanas antes de una rotación, luego se crearán nuevos archivos log, para el archivo rotado se usara un sufijo con la fecha de rotación.

```

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    minsize 1M
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 1
}

# system-specific logs may be also be configured here.

```

Video tutorial (actividad3): <https://www.youtube.com/watch?v=cXf9ubHHArM&feature=youtu.be>