

Administración de Sistemas Operativos



U11. Monitorización (Linux)



U11. Monitorización (Linux)

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

HERRAMIENTAS BÁSICAS



U11. Monitorización (Linux)

Elementos a monitorizar

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

- **Procesos.** Muestra información sobre los procesos que se están ejecutando en el sistema.

ps

- **Almacenamiento.** Proporcionan información sobre la entrada y salida al subsistema de almacenamiento.

df, du

- **Memoria.** Proporcionan información sobre el espacio de memoria real y *swap*.

free, pmap

- **Red.** Facilitan estadísticas de uso de las interfaces de red.

Ifstat, iftop, iptraf, netstat, ping, traceroute

- **Polivalentes.** Muestran información sobre distintos subsistemas del equipo.

dstat, iostat, top, vmstat, who, xosview



U11. Monitorización (Linux)

Elementos a monitorizar

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

df

```
root@www:~  
Archivo  Editar  Ver  Terminal  Ir a  Ayuda  
[root@www root]# df  
S.ficheros      1K-blocks      Used Available Use% Montado en  
/dev/hda2      15891788      3351600 11732924  23% /  
/dev/hda1       101089        9324    86546    10% /boot  
none           127124         0      127124    0% /dev/shm  
[root@www root]#
```

iptraf

```
root@adminiso:~  
Archivo  Editar  Ver  Terminal  Solapas  Ayuda  
IPTraf  
TCP connections (Source Host:Port)  Packets  Bytes  Flags  Iface  
150.214.153.140:22 > 224 48224 -PA- eth0  
150.214.154.15:2461 > 117 5592 --A- eth0  
150.214.153.140:80 > 3 3836 --A- eth0  
201.223.11.229:63367 > 5 511 DONE eth0  
150.214.153.140:80 > 4 5988 --A- eth0  
201.223.11.229:63275 > 4 465 CLOSED eth0  
201.223.11.229:62995 = 2 96 S--- eth0  
150.214.153.140:80 = 4 192 S-A- eth0  
201.223.11.229:62047 > 1 46 --A- eth0  
150.214.153.140:80 > 2 4436 --A- eth0  
201.223.11.229:62651 > 2 92 --A- eth0  
150.214.153.140:80 > 1 1492 --A- eth0  
TCP: 28 entries Active  
UDP (78 bytes) from 150.214.153.225:59646 to 150.214.153.255:137 on eth0  
UDP (78 bytes) from 150.214.153.225:59645 to 150.214.153.255:137 on eth0  
UDP (78 bytes) from 150.214.153.225:59645 to 150.214.153.255:137 on eth0  
UDP (78 bytes) from 150.214.153.225:59645 to 150.214.153.255:137 on eth0  
UDP (229 bytes) from 150.214.153.231:138 to 150.214.153.255:138 on eth0  
Packets captured (all interfaces): 604 | TCP flow rate: 20.40 kbits/s  
Up/Dn/PgUp/PgDn-scroll M-more TCP info W-chg actv win S-sort TCP X-exit
```



U11. Monitorización (Linux)

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

DIRECTORIO /PROC



U11. Monitorización (Linux)

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

El núcleo de Linux almacena información relativa a su funcionamiento en archivos situados en el directorio /proc, de tal forma que, para analizar el comportamiento de un sistema, también se puede recurrir a la consulta de los archivos de este sistema de ficheros.

```
[root@ejemplo root]# cat /proc/meminfo
          total:      used:      free:  shared: buffers:  cached:
Mem:  129015808 124686336  4329472           0 12189696 65392640
Swap: 534634496  5824512 528809984
MemTotal:        125992 kB
MemFree:          4228 kB
MemShared:         0 kB
Buffers:         11904 kB
Cached:          61772 kB
SwapCached:       2088 kB
Active:           88364 kB
ActiveAnon:       33868 kB
ActiveCache:      54496 kB
Inact_dirty:        56 kB
Inact_laundry:    19124 kB
Inact_clean:       1076 kB
Inact_target:     21724 kB
HighTotal:         0 kB
HighFree:          0 kB
LowTotal:         125992 kB
LowFree:           4228 kB
SwapTotal:        522104 kB
SwapFree:         516416 kB
[root@ejemplo root]#
```

Contenido del fichero /proc/meminfo.



U11. Monitorización (Linux)

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

ARCHIVOS DE REGISTRO - SYSLOG -



U11. Monitorización (Linux)

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

En los archivos de registro se va almacenando toda la actividad que realiza el sistema. Existen muchos motivos por los que se pueden generar mensajes. Entre los más frecuentes se encuentran los fallos del servidor (p.e.: problema de hardware, fallo en un servicio), de autenticación (p.e.: fallo en la autenticación de un usuario) o por la utilización de un servicio (p.e.: petición de un cliente de una página web).

```
root@master:/var/log# ls
alternatives.log  bttmp          dmesg.3.gz    lastlog        pycentral.log
apache2           daemon.log     dmesg.4.gz    lpr.log        syslog
apparmor          debug          dpkg.log      mail.err       udev
apt               dist-upgrade   faillog       mail.info      ufw.log
aptitude          dmesg          fsck           mail.log       unattended-upgrades
auth.log          dmesg.0        installer     mail.warn      user.log
boot              dmesg.1.gz    iptraf        messages       wtmp
boot.log          dmesg.2.gz    kern.log      news
```

```
root@master:/var/log# _
```




U11. Monitorización (Linux)

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

Estos mensajes se pueden encontrar en el directorio /var/log. Por ejemplo, muchos mensajes son reportados en los ficheros /var/log/syslog o en el /var/log/messages. Pero si un servicio genera muchos mensajes lo normal es que sean escritos en un fichero o carpeta separada como lo hace apache (/var/log/apache2).

Apache2
Directorio de registro del servidor web

Messages
Mensajes generales del sistema

```
root@master:/var/log# ls
alternatives.log  bttmp          dmesg.3.gz    lastlog        pycentral.log
apache2           daemon.log     dmesg.4.gz    lpr.log        syslog
apparmor          debug          dpkg.log       mail.err       udev
apt               dist-upgrade   faillog        mail.info      ufw.log
aptitude          dmesg          fsck           mail.log       unattended-upgrades
auth.log          dmesg.0        installer      mail.warn      user.log
boot              dmesg.1.gz    iptraf         messages       wtmp
boot.log          dmesg.2.gz    kern.log       news
```



U11. Monitorización (Linux)

syslog

Contenido

Herramientas
básicas

Directorio /proc

Archivos de
registro

El registro de todos los mensajes del sistema lo realiza el servicio syslogd (o rsyslogd), el cuál no es exclusivo de los servicios del sistema sino que nosotros también puede registrar sus propios mensajes usando syslog.

Es posible personalizar el comportamiento de syslog para indicar los registros que quieres guardar.



