Administración de Sistemas

3 - Control de la configuración en Linux

Diciembre 2003

Guillermo Pérez Trabado

Dept. Arquitectura de Computadores

Universidad de Málaga

Arranque del sistema

- El sistema usa un conjunto de scripts (ficheros de texto con comandos) para arrancar todos los servicios. La mayor parte de ellos están bajo el directorio /etc/rc.d o /etc/init.d según la versión de UNIX en que estemos (en RedHat es /etc/rc.d).
- El primer script que se ejecuta después de cargar el nucleo es /etc/rc.d/rc.sysinit
- Este script hace las tareas más básicas de inicialización y consulta si hemos puesto el argumento “single” en el arranque para abrir una consola y permitirnos administrar (modo **single user**).
- El modo “single user” permite administrar un sistema que no arranca. Equivalente al “A prueba de fallos” en Windows.
- A continuación decide un nivel de arranque (runlevel) y se arrancan los servicios para dicho nivel.

Runlevel

- Existen 7 niveles (de 0 a 6).
- El runlevel identifica un estado de funcionamiento del sistema. Parecido a un perfil.
- Algunos niveles están predefinidos:
  - 0: Sistema apagado.
  - 1: Sistema en modo “single user”. No pueden entrar usuarios.
  - 2: Sistema en marcha con red activada pero sin exportar o importar discos a través de la red.
  - 3: Sistema totalmente operativo. (Linux: Entorno gráfico desactivado).
  - 4: Definible por el administrador.
  - 5: Definible por el administrador. (Linux: “nivel 3”+Entorno gráfico activado).
  - 6: Reinicio del sistema.
- El runlevel por defecto del sistema se define en /etc/inittab

  ```
  id:3:initdefault:
  ```
- Se puede cambiar el nivel interactivamente con el comando:

  ```
  $ telinit n
  ```

Arranque de los servicios

- Cada servicio a arrancar está representado por un script con la secuencia de comandos para arrancar y parar el mismo. Debe aceptar obligatoriamente los argumentos “start” y “stop”.
- Se pueden usar manualmente como administrador ejecutando el script con dichas opciones.
- Para cada runlevel hay un directorio que contiene todos los scripts que se han de ejecutar al cambiar a dicho nivel.
  - /etc/rc.d/rc0.d , /etc/rc.d/rc1.d , ... , /etc/rc.d/rc6.d
- El nombre del script debe comenzar por S*nn*NOMBRE o K*nn*NOMBRE donde *nn* son dos dígitos, que permite ordenar la ejecución de los scripts de 00 a 99.
- Si comienza por ‘S’ se ejecuta con la opción “start”. Con ‘K’ se ejecuta con la opción “stop”. Primero se ejecutan todas las ‘K’ y luego todas las ‘S’.
- Para no replicar los scripts, en realidad son enlaces simbólicos al directorio /etc/init.d o /etc/rc.d/init.d según versión de UNIX.

Añadiendo y quitando servicios

- Para definir los servicios que se arrancan y paran en cada nivel hay que crear o borrar soft-links en cada directorio rc*N*.d
- Para facilitar esto, cada script lleva un comentario en su cabecera definiendo el número de orden *nn* y los niveles en que arranca.

```
$ more /etc/rc.d/init.d/smb
#!/bin/sh
#
# chkconfig: 345 91 35
# description: Starts and stops the Samba smbd and nmbd daemons
```

- El comando chkconfig lee este comentario y crea o borra los soft-links.

```
$ chkconfig --add smb → Añade los softlinks.
$ chkconfig --del smb → Quita los softlinks.
```

- Para ver todos los servicios usamos

```
$ chkconfig --list
```

- Si el comentario tiene un guión en la lista de niveles, no se crean los links aunque usemos “chkconfig --add”. ¡Servicios peligrosos!
- Los servicios se arrancarán la próxima vez que se inicie el sistema.

Los servicios de red (inetd)

- Hay servicios que solo se arrancan cuando son accedidos desde la red.
- El daemon “xinetd” se ocupa de recibir las peticiones y de arrancar los procesos correspondientes.
- Requiere una lista de servicios para traducir:

  “puerto TCP/UDP” → “proceso a ejecutar”
- Cada servicio consiste en un fichero en el directorio /etc/xinetd.d
- Cada fichero define todos los parámetros de un servicio.

```
$ more /etc/xinetd.d/telnet
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = yes
}
```

Añadiendo y quitando servicios de inetd

- La opción “disable = yes” en cada fichero permite deshabilitar un servicio sin borrar el fichero de control.

- Si se edita un fichero (o más) hay que reiniciar el daemon xinitd con el comando para que los cambios sean efectivos sin reiniciar el sistema.

```
$ service xinetd restart
```

- Por seguridad, casi todos los servicios están deshabilitados.

- “Xinetd” sustituye al antiguo “inetd” que usaba el fichero /etc/inetd.conf (en algunos sistemas UNIX todavía está presente).

Control del acceso al sistema

- TCP Wrapper
  - Filtro de conexiones para inetd.
  - Se controla mediante los ficheros /etc/hosts.allow y /etc/hosts.deny.
  - Actualmente hay muchas aplicaciones que integran en su código el control y no necesitan el uso de tcpwrapper.
- Xinetd
  - Incorpora capacidades de control de acceso.
  - Se definen:
    - Por defecto para todos los servicios en /etc/xinetd.conf
    - Especificas para un servicio en /etc/xinetd.d/<servicio>
- Otras aplicaciones
  - Usan la librería tcpwrapper en su código.
  - Definen el control de acceso en su propia configuración.
  - Por ejemplo: SAMBA.

Control de Xinetd

- Si el fichero /etc/xinetd.conf no contiene ninguna línea "*only_from*" no hay control de acceso global.
- En caso contrario define la lista de direcciones que pueden acceder a todos los servicios:
- En caso contrario define la lista de direcciones que pueden acceder a

```
only_from                    = 150.214.109.2 172.16.52.0/24
```

- Se pueden especificar direcciones individuales o rangos. Para los rangos se añade el número de bits a 1 de la máscara:
  - 172.16.52.0/24 ~ red: 172.16.52.0, máscara 255.255.255.0
  - 172.16.52.0/25 ~ red: 172.16.52.0, máscara 255.255.255.128
  - 0.0.0.0/0 ~ **cualquier dirección IP**
- Si se incluye la línea "*only_from*" en un fichero de definición de un servicio (/etc/xinetd.d/<servicio>), la lista del servicio prevalece sobre la lista por defecto.