INGENIERÍA DE SERVIDORES (2016-2017)
GRADO EN INGENIERÍA INFORMÁTICA
UNIVERSIDAD DE GRANADA

Memoria Práctica 5

Adrián Morente Gabaldón

19 de enero de 2017

Índice

Índice de figuras

Índice de tablas

1. [SYSCTL] Al modificar los valores del kernel de este modo, no logramos que persistan después de reiniciar la máquina. ¿Qué archivo hay que editar para que los cambios sean permanentes?

Como ya se explicó en clase de prácticas, *Sysctl* modifica los parámetros del kernel en tiempo de ejecución, por lo que al reiniciar la máquina se pierden los valores modificados. Si ejecutamos Sysctl a través de línea de comandos sin opciones, se nos despliega una pequeña lista con sus opciones más destacadas, que son las siguientes:

```
(lun dic 26-13:47:16)-[adri@ubuntuserver:~]$ sysctl

Usage:
 sysctl [opciones] [variable[=valor] ...]

Options:
  -a, --all            mostrar todas las varaibles
  -A                   alias de -a
  -X                   alias de -a
      --deprecated     incluir parámetros obsoletos en la lista
  -b, --binary         mostrar valor sin nueva línea
  -e, --ignore         ignorar errores de variables desconocidas
  -N, --names          mostrar nombres de variables sin valores
  -n, --values         mostrar solo valores de las variables
  -p, --load[=<archivo>]  leer valores de archivo
  -f                   alias de -p
      --system         leer valores de todos los directorios de sistema
  -r, --pattern <expresión>
                       seleccionar configuración que cumple con la expresión
  -q, --quiet          no mostrar eco al establecer la variable
  -w, --write          activar escritura de un valor a variable
  -o                   no hace nada
  -x                   no hace nada
  -d                   alias de -h

 -h, --help     display this help and exit
 -V, --version  output version information and exit

For more details see sysctl(8).
```

Figura 1.1: Opciones más destacadas de sysctl. - Adrián Morente Gabaldón [26/12/2016]

Como vemos en la captura de pantalla anterior, el propio sysctl nos redirige a su manual si queremos explorar más opciones u obtener más información. Al principio de este manual, encontramos que todos los parámetros configurables descienden del directorio */proc/sys*, ordenados en subcarpetas según pertenencia (sistema de archivos, kernel, memoria virtual, etc), y cada uno de ellos se encuentra en formato de archivo en texto plano, conteniendo tan solo el valor del parámetro en cuestión. Veamos un ejemplo de los parámetros pertenecientes al módulo de memoria virtual:

```
(mié dic 28-10:20:40)-[adri@ubuntuserver:~]$ ls /proc/sys
abi  debug  dev  fs  kernel  net  vm
(mié dic 28-10:20:47)-[adri@ubuntuserver:~]$ ls /proc/sys/vm
admin_reserve_kbytes         laptop_mode                oom_dump_tasks
block_dump                   legacy_va_layout           oom_kill_allocating_task
compact_memory               lowmem_reserve_ratio       overcommit_kbytes
compact_unevictable_allowed  max_map_count              overcommit_memory
dirty_background_bytes       memory_failure_early_kill  overcommit_ratio
dirty_background_ratio       memory_failure_recovery    page-cluster
dirty_bytes                  min_free_kbytes            panic_on_oom
dirty_expire_centisecs       min_slab_ratio             percpu_pagelist_fraction
dirty_ratio                  min_unmapped_ratio         stat_interval
dirtytime_expire_seconds     mmap_min_addr              swappiness
dirty_writeback_centisecs    nr_hugepages               user_reserve_kbytes
drop_caches                  nr_hugepages_mempolicy     vfs_cache_pressure
extfrag_threshold            nr_overcommit_hugepages    zone_reclaim_mode
hugepages_treat_as_movable   nr_pdflush_threads
hugetlb_shm_group            numa_zonelist_order
(mié dic 28-10:20:48)-[adri@ubuntuserver:~]$ cat /proc/sys/vm/laptop_mode
0
```

Figura 1.2: Contenido del directorio /proc/sys, sus subdirectorios y ejemplo de uno de sus parámetros. - Adrián Morente Gabaldón [28/12/2016]

Para que los cambios persistan tras reiniciar la máquina, debemos aplicar la modificación a cada uno de los ficheros de parámetros. Sin embargo, por temas de seguridad, es mejor utilizar esta herramienta con algunas de sus múltiples opciones en lugar de acceder y modificar directamente dichos ficheros (ya que podemos "tocar donde no debemos"), cosa que podría derivar en algún fallo no deseado del sistema. Como vimos en clase, y como bien comenta el manual de *sysctl*, la configuración perteneciente y valorable por esta herramienta se encuentra principalmente en el archivo /etc/sysctl.config, y colgando del directorio /etc/sysctl.d. Veamos una parte del contenido de dicho primer archivo:

```
(jue ene 19-10:20:09)-[adri@ubuntuserver:/]$ cat /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

##############################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
```

Figura 1.3: Parte del contenido del archivo de configuración /etc/sysctl.config. - Adrián Morente Gabaldón [19/01/2017]

Como podemos apreciar, no encontramos mucha información sobre qué es cada cosa, solo encontramos nombres de variables con sus correspondientes valores; todos ellos ordenados de forma clara y precisa según su ámbito. Por ejemplo, veamos uno de estos ámbitos que, personalmente, me ha llamado la atención, y es el relacionado con la **seguridad** del sistema:

Figura 1.4: Contenido del archivo de configuración /etc/sysctl.config relacionado con la seguridad del sistema. - Adrián Morente Gabaldón [19/01/2017]

En este apartado, encontramos parámetros configurables que nos permitirían en cierto modo evitar algunos ataques a nuestro sistema, como pueden ser el bloqueo de redirecciones mediante el protocolo ICMP (que incluye herramientas como ping o traceroute, como hemos visto en la asignatura de *Fundamentos de Redes*). Como bien explica la pequeña introducción en este apartado, estas son medidas contra el *spoofing* (que en español se traduce por *burla* o *engaño*, y en informática entendemos por "falsificación de identidad") y contra ataques *Man In The Middle*, término que ya conocemos.
Para terminar, cabe destacar que todos estos últimos parámetros están comentados, de forma que el sistema toma valores por defecto en lugar de los especificados aquí. Las instrucciones del archivo nos instan a no modificar parámetros si no sabemos lo que estamos haciendo. Además, ya sabemos que en caso de tener que modificarlos, debemos hacer copia de seguridad previa a su modificación.

2. ¿Con qué opción se muestran todos los parámetros modificables en tiempo de ejecución? Elija dos parámetros y explique, en dos líneas, qué función tienen.

Si leemos el manual de sysctl en la terminal, vemos rápidamente que la opción para consultar todas las variables modificables en ejecución es *-a*:

```
-a, --all
       Display all values currently available.
```

Figura 2.1: Opción de Sysctl para consultar los parámetros modificables en ejecución. - Adrián Morente Gabaldón [26/12/2016]

Si ejecutamos **sysctl -a** obtenemos una extensa lista con todas las variables configurables. Exactamente, tantas como ficheros había en los subdirectorios de */proc/sys* vistos en el ejercicio anterior, lógicamente.

3. [Windows Server] a) Realice una copia de seguridad del registro y restáurela, ilustre el proceso con capturas. b) Abra una ventana mostrando el editor del registro.

Para empezar, seguiremos las instrucciones dictadas por el guión de prácticas, comenzando por ejecutar *regedit* desde la línea de comandos de Windows Server. A continuación, nos encontraremos con esta ventana:

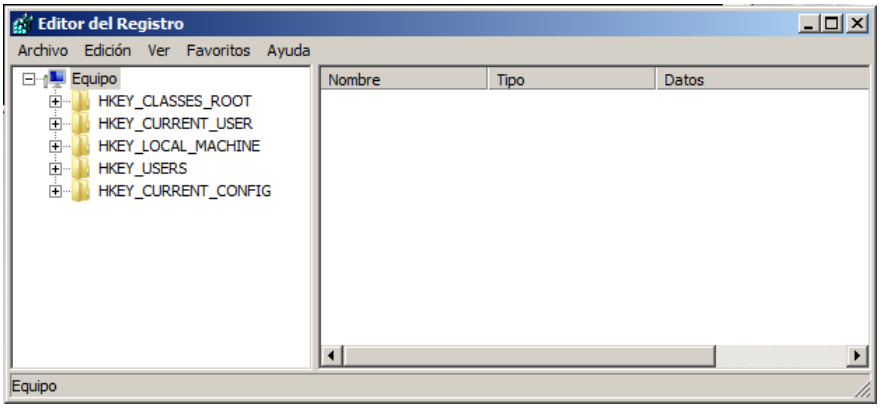

Figura 3.1: Ventana principal del Editor del Registro en Windows Server. - Adrián Morente Gabaldón [26/12/2016]

4. Enumere qué elementos se pueden configurar en Apache y en IIS para que Moodle funcione mejor.

5. Ajuste la compresión en el servidor y analice su comportamiento usando varios valores para el tamaño de archivo a partir del cual comprimir. Para comprobar que está comprimiendo puede usar el navegador o comandos como curl (see url) o lynx. Muestre capturas de pantalla de todo el proceso.

6. a) Usted parte de un SO con ciertos parámetros definidos en la instalación (Práctica 1), ya sabe instalar servicios (Práctica 2) y cómo monitorizarlos (Práctica 3) cuando los somete a cargas (Práctica 4). Al igual que ha visto cómo se puede mejorar un servidor web (Práctica 5 Sección 3.1), elija un servicio (el que usted quiera) y modifique un parámetro para mejorar su comportamiento. b) Monitorice el servicio antes y después de la modificación del parámetro aplicando cargas al sistema (antes y después) mostrando los resultados de la monitorización.

7. PREGUNTAS OPCIONALES

7.1. Realice lo mismo que en la cuestión 6 pero para otro servicio.

8. PREGUNTAS OPCIONALES DE PRÁCTICAS ANTERIORES