Curso de Introducción a la Informática

Práctica:	**MAC: ADMINISTRACIÓN Y AUDITORÍA**
Profesor:	Héctor Menéndez
Departamento:	Ingeniería Informática
Centro:	Escuela Politécnica Superior
Curso:	2012/13
Tiempo estimado:	30 min

Objectivos y Descripción

El objetivo de esta práctica es adquirir una serie de conocimientos más avanzados sobre la administración y auditoría de un Sistema Operativo MAC OS.

Estos ejemplos muestran una serie de características que complementan en gran medida los conocimientos adquiridos en la parte sobre linux (dada la alta compatibilidad) pero enfocado más hacia un entorno gráfico más amigable para el usuario que al entorno de terminal.

El guión servirá para poder ver de forma continuada como se pueden utilizar estas herramientas.

Desarrollo

Para entender de forma avanzada cómo administrar y auditar un Sistema Operativo MAC, es necesario ver cómo el usuario puede acceder de forma más profunda a la información del sistema. Para ello se utilizarán herramientas que faciliten información sobre: procesos, usuarios, red.

Logs del sistema

El sistema almacena todos los mensajes emitidos por los distintos procesos que se están ejecutando en logs. Estos mensajes facilitan información sobre puertos que se abren o programas que se conectan a la red, errores producidos durante la ejecución de un programa, gravedad de estos errores, etc.

Para poder leer estos mensajes, Mac OS facilita una interfaz de usuario denominada consola donde muestra la lista de errores emitidos en formato log, permitiendo, entre otras cosas, realizar una búsqueda de los errores producidos durante la ejecución. La Figura 1 muestra un ejemplo de estos errores.

Ejercicio 1. *Abrir la aplicación de Consola y ver los mensajes de error que se han producido.*

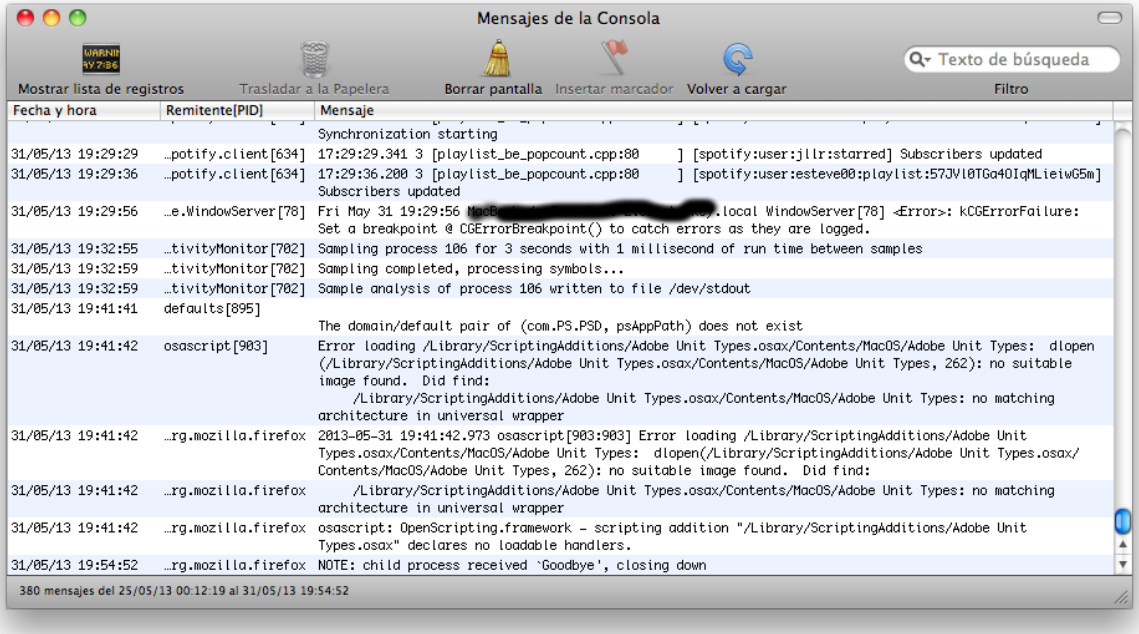

Figura 1: Ejemplo de la Interfaz del Perfil del Sistema

Monitorización de Procesos

Al igual que el resto de los sistemas operativos UNIX, MAC divide sus distintas actividades en procesos y subprocesos. Éstos son a su vez generados a partir de otros procesos que los lanzan, descendiendo todos ellos de un proceso inicial generado por el usuario administrador o `root`. El proceso inicial que carga el núcleo del sistema operativo se denomina `kernel_task` y el proceso que se dedica a lanzar procesos se denomina `launchd`.

Para poder hacer un seguimiento de cuántos procesos está ejecutando cada usuario del sistema operativo, se puede utilizar el Monitor de Actividad. Éste aporta información sobre el ID de cada proceso, el nombre, el usuario que lo ha lanzado, el porcentaje de CPU que está utilizando en ese momento, cuántos subprocesos está ejecuntado y qué memoria RAM está gastando. Además, el monitor muestra unas estadísticas de uso de la CPU por núcleo, de la memoria, de los discos y de la red.

La Figura 2 muestra un ejemplo de la interfaz del Monitor de Actividad.

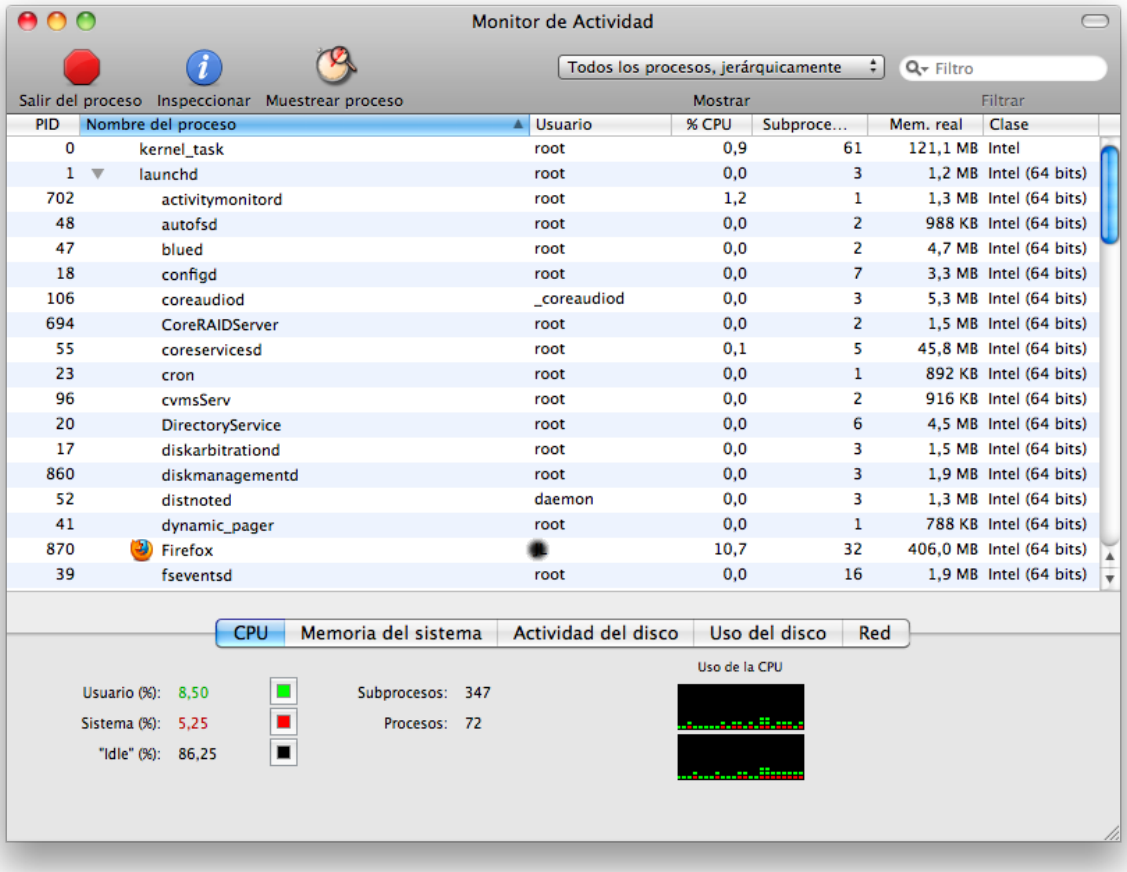

Figura 2: Ejemplo de la Interfaz del Perfil del Sistema

Ejercicio 2. *Ver las distintas funciones del Monitor de Actividad.*

Aparte, el Monitor de Actividad permite inspeccionar un proceso en concreto adquiriendo una información más detalla del mismo y realizar un muestreo de las distintas llamadas que está realizando dicho proceso. Este muestreo genera un árbol de llamadas.

La Figura 3 muestra un ejemplo del proceso de muestreo de un proceso.

Ejercicio 3. *Realizar la muestra de un determinado proceso.*

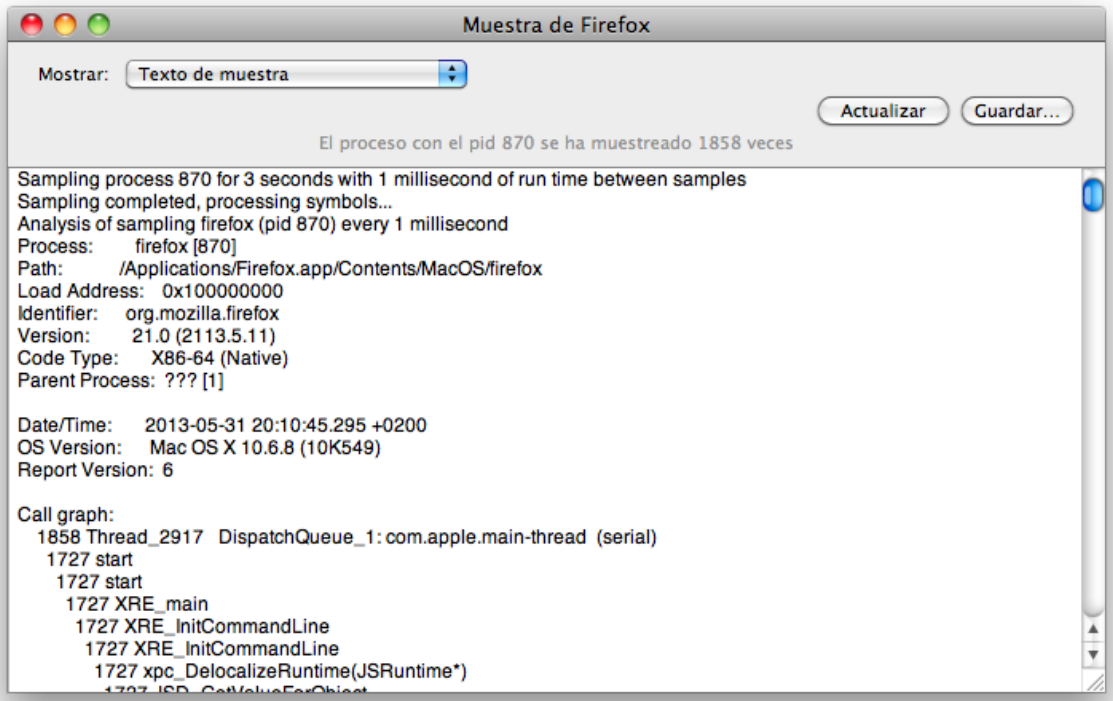

Figura 3: Ejemplo de la Interfaz de Muestra de un proceso

Terminal

AL igual que todos los sistemas UNIX, MAC también dispone de una terminal que permite realizar varias operaciones. Muchos de los comandos son muy similares a los comandos vistos en Linux, pero hay una serie de diferencias importantes, sobre todo en la gestión de usuarios.

Administración remota

Al igual que en los sistemas Linux, la administración del sistema puede realizarse de forma remota. En esta práctica se verá como activar la sesión remota para gestión por `ssh`.

Mac OS ya está preparado para soportar gestión remota, pero por defecto no está activada. Esta se activa en la sección 'Compartir' de las 'Preferencias del Sistema'. La Figura 4 muestra el panel para activar la sesión remota.

Ejercicio 4. *Activar la sesión remota y probar a conectarse a* `localhost`.

Figura 4: Panel para activar la sesión remota

Auditoría

Al igual que en los sistemas Linux, Mac OS permite utilizar la herramienta `audit` para realizar auditoría del sistema, aunque hay distintas variaciones en los comandos.

El fichero `/var/audit` contiene los logs del sistema de auditoría. Los nombres de los ficheros contienen la fecha y hora de cuándo fueron creados y cerrados, por ejemplo, el fichero '20040322183133.20040322184443' fue creado el 22 de Marzo de 2004 a las 18:31:33 y cerrado el 22 de Marzo de 2004 a las 18:44:43. Para ver el contenido de los ficheros, se puede utilizar: `praudit`. Por ejemplo:

```
> praudit -l /var/audit/20040322183133.20040322184443
```

Permite ver el fichero seleccionado. Si además se desea ver información más específica de un usuario concreto, se utiliza, `auditreduce`. Esto muestra información más específica de eventos, usuarios o tiempos. Por ejemplo, para ver información sobre el usuario `root` se puede utilizar:

```
> auditreduce -e root /var/audit/20040322183133.20040322184443
```

También se puede utilizar `auditd` para seguir más eventos. La lista completa de posibles clases de eventos se puede encontrar en `/etc/security/audit_class` y la lista completa de eventos y sus llamadas al sistema en `/etc/security/audit_event`. Para más información ver la páginas de `man` de `audit_control` and `audit_event`.

Ejercicio 5. *Elegir un fichero de* `/var/audit` *y decir en qué fecha se ha creado y cerrado y utilizar los comandos* `praudit` *para leerlo y* `auditreduce` *para buscar información de acceso de algún usuario.*