Monitorización de cambios en ficheros

Grupo de laboratorio 41

Carlos Sánchez Velázquez

Sumit Kumar Jethani Jethani

20/01/2021

Introducción

Esta práctica consiste en la elaboración de scripts para monitorizar el contenido de los directorios almacenados en un fichero de configuración y comprobar si se han producido cambios en los ficheros de esos directorios con respecto a la configuración original. Dicha comprobación, se lleva a cabo semanalmente, en nuestro caso, cada domingo a las 12.

Script snapshot

Este script, se encarga de obtener una foto /Snapshot/snapshot del estado de los ficheros de cada uno de los directorios de un fichero de configuración, en la configuración inicial, foto que contendrá en cada línea el nombre de un directorio del fichero de configuración, separado por un ";" de una lista de los ficheros contenidos en este, separados por ";" cada uno de estos, seguido de sus permisos y su suma de control (sha512) separados por "," por ejemplo:

/root;fichero1,permisos1,checksum1;fichero2,permisos2,checksum2;

En el caso de que un fichero sea de tipo directorio, bloque o carácter, o enlace simbólico, no se calcula la suma de comprobación de estos, por tratarse de ficheros especiales del sistema.

El formato de invocación de este script es el siguiente:

./snapshot.sh [-c] [ficheroDeConfiguracion]

-c: Opción adicional que realiza la limpieza del directorio /Snapshot (eliminando versiones antiguas de la foto)

ficheroDeConfiguracion: Fichero que contiene en cada línea un directorio a monitorizar, que, en caso de su ausencia, se toma el fichero por defecto /root/Monitorización_de_ficheros/config_file

Además, si ya existe alguna foto previa con el nombre snapshot en el directorio /Snapshot, se le cambia el nombre por snapshot.dd-mm-yyyy-HH:MM:SS

Script compare_snapshot

El objetivo de este script, es comparar la foto original tomada, con el contenido actual de los directorios especificados en el fichero de configuración. En un primer lugar, se comprueba que todos los directorios que aparecen en el fichero de configuración se encuentran en la foto tomada, en caso contrario se notifica un error, indicando el directorio que no existe en la foto, y abortando. En caso de que coincidan todos los directorios, se notificarán en fichero /var/log/binchecker las siguientes posibles 4 diferencias entre los ficheros actuales de estos directorios y los contenidos en la foto:

- Archivos suprimidos
- Nuevos archivos añadidos
- Cambios de permisos en los archivos existentes
- Cambios en el contenido de los contenidos existentes

El formato de invocación de este script es el siguiente:

./compare_snapshot [ficheroDeConfiguracion]

ficheroDeConfiguracion: Fichero que contiene en cada línea un directorio a monitorizar, que, en caso de su ausencia, se toma el fichero por defecto /root/Monitorización_de_ficheros/config_file

Para ejecutarse estos scripts semanalmente, los domingos a las 12:00, los hemos programado para ejecutarse por medio de la utilidad crontab del sistema, como se ve en la siguiente captura.

```
[root@localhost Monitorizacion_de_ficheros]# cat copia_crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
0 0 * * 0 root /root/Monitorizacion_de_ficheros/snapshot.sh; /root/Monitorizacion_de_ficheros/compare_snapshot.sh
[root@localhost Monitorizacion_de_ficheros]#
```