Apuntes de bash, sed, awk para administradores

A veces hay que analizar, extrare datos de los logs (benditos logs) y viene bien una chuleta a mano, para los que no estamos todo el día con el sistema, o la memoria muy floja por la edad.

- Básicos de sed
- Eliminar la extensión de ficheros para procesos en lote bash
- Guía de Comando `find` - Especialidad para Sysadmin

Básicos de sed

Eliminar comentarios y lineas en blanco con sed (bash o zsh)

Correción realziada el 22/08/2024 ~~sed '/^\s*#/d' file_original.txt~~

```
sed '/^\s*#/d;/^\s*$/d' file_original.txt
```

Eliminar de un fichero todo menos una cadena (csf.deny)

) Una comando muy útil cuando queremos, por ejemplo, vaciar el csf.deny salvo las lineas que contiene un cadena "do not delete" o similar

```
sed -i '/do not delete/!d' /etc/csf/csf.deny
## O la de abajo segun configuraciones
sed -i -e '/do not delete/!d' /etc/csf/csf.deny
```

Aviso

Eliminar la extensión de ficheros para procesos en lote bash

Introducción

Alguna vez uno tiene que hacer cositas, en el que queremos restaurar un lote de ficheros de backups cuyo formato es `nombre_de_usuario.tar.gz` pero el script para hacer el restore requiere el nombre del usuario y no el nombre de fichero

Eliminar la extnesón de ficheros tar.gz

```
ls | sed -n '/\.tar\.gz$/s///p'
```

Asi nos quedaria algo asi.

```
for user in $(ls *.tar.gz | sed -n '/\.tar\.gz$/s///p'); do echo $user; command $user; done
```

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como esta, sin que ello implique ningún obligación ni responsabilidad por parte de Castris

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

Guía de Comando `find` - Especialidad para Sysadmin

Introudcción

Como sysadmin experimentado, sabes que `find` es una navaja suiza. Aquí tienes los patrones más útiles, organizados por casos de uso prácticos:

Limpieza por Antigüedad

Archivos más antiguos de X días:

```
# Ver qué se borraría (siempre prueba primero)
find /ruta -type f -mtime +30 -ls

# Borrar archivos de más de 30 días
find /ruta -type f -mtime +30 -delete

# Más seguro: con confirmación
find /ruta -type f -mtime +30 -ok rm {} \;
```

Por horas (útil para logs):

```
# Archivos de más de 24 horas
find /var/log -type f -mmin +1440 -delete

# De más de 2 horas
find /tmp -type f -mmin +120 -delete
```

Limpieza por Tamaño

Archivos grandes:

```
# Archivos de más de 100MB
find /ruta -type f -size +100M -ls

# Mayores de 1GB
find /ruta -type f -size +1G -delete

# Combinar: grandes Y antiguos
find /ruta -type f -size +50M -mtime +7 -delete
```

Archivos vacíos:

```
# Archivos de 0 bytes
find /ruta -type f -empty -delete

# Directorios vacíos
find /ruta -type d -empty -delete
```

Patrones de Limpieza Combinados

El combo perfecto para /tmp:

```
find /tmp -type f \( -mtime +7 -o -size +500M \) -delete
```

Logs rotativos:

```
# Solo .log antiguos, preservar los .gz
find /var/log -name "*.log" -mtime +30 -delete
```

Core dumps y temporales:

```
# Múltiples patrones
find /ruta \( -name "core.*" -o -name "*.tmp" -o -name "*.temp" \) -mtime +1 -delete
```

Modificadores de Tiempo Útiles

- `-mtime +N` : modificado hace MÁS de N días
- `-mtime -N` : modificado hace MENOS de N días
- `-mtime N` : modificado hace EXACTAMENTE N días

- `-atime` : último acceso
- `-ctime` : cambio de metadatos

Consejos de Veterano

Siempre prueba primero:

```
# Reemplaza -delete por -ls para ver qué haría
find /ruta -criteria -ls
```

Para grandes volúmenes, usa xargs:

```
find /ruta -type f -mtime +30 -print0 | xargs -0 rm
```

Excluir directorios específicos:

```
find /var -path "/var/lib" -prune -o -type f -mtime +30 -delete
```

La clave está en la combinación de criterios. El `find` permite ser muy preciso, pero siempre con la prudencia que dan los años de experiencia.

Aviso