

Cibernarium Linux 1

[linux](#), [cursos](#)

datos

- 13/11/2012
- Ramón Soler (empresa dedicada conversión a software libre)

resumen

componentes distribución linux

- kernel
- boot manager
- interfaz usuario
 - GUI - gráfico
 - CLI - línea de comandos
- X Window
- Red e Internet
- Impresión → CUPS
- Gestión de paquetes
- Herramientas/Lenguajes de programación
- librerías
- Herramientas administración
- aplicaciones

conceptos fundamentales

- GUI, CLI
- Multiusuario
- SWAP
- Filesystem jerárquico
- Ejecutables
- Directorio raíz (/)
- usuario root
- directorio home
- montaje dispositivos
- niveles de ejecución
- cierre de sistema

particionado

- de SWAP
- de S.O.
- de Datos de Usuario

Formateo y montaje

- File System → organización de ficheros
- SWAP, BDD (Oracle) → gestión propia del disco, sin FileSystem
 - el tamaño del SWAP, actualmente, la misma que la física (equipos superdimensionados)
 - es posible crear un fichero en filesystem para usar como SWAP

características

- multitarea
- multiusuario
- multiplataforma
- multiprocesador
- multithreading
- memoria protegida entre procesos
- carga de ejecutables bajo demanda
- memoria virtual para paginación (no por procesos)
- librerías dinámicas compartidas bajo demanda
- consolas virtuales múltiples
- soporte múltiples sistemas de archivos

filesystem

- / → raíz del sistema de archivos
- /root → home del usuario root
- /home/«user» → directorios home de los usuarios
- /usr → «home» de las aplicaciones, configuraciones, librerías
- /bin, /usr/bin → ejecutables
- /sbin, /usr/sbin → ejecutables de sistema
- /opt → aplicaciones??
- /etc → configuraciones del sistema
- /var → espacio de archivos variables (colas de impresión, logs, spools...)
- /boot → archivos de arranque (bootloader)

bootloader

- niveles de ejecución:
 - 5 → single user minim
 - 1 → single user normal
 - 2 → multiusuario sin red
 - 3 → multiusuario con red
 - 4 → reservado
 - 5 → multiusuario con red y GUI
 - 6 → reboot
 - 0 → shutdown
- \$ init
- \$ runlevel
- debían cambiar los niveles de ejecución, arrancando todo en nivel 3, arrancado en función de otros ficheros de configuración

sistema de usuarios

- sistema multiusuario
 - compartir recursos
 - sistema de seguridad para evitar acceso a recursos no autorizados

- login
 - primer sistema de seguridad
 - para poder acceder al sistema
 - los usuarios se listan en `/etc/passwd`
 - se pueden ocultar las contraseñas del fichero `/etc/passwd` en el fichero `/etc/shadow` (de solo acceso para root)
 - shell (concha) con la que interacciona el usuario (línea de comandos)
 - `/bin/false` → para evitar acceso interactivo, sin shell
 - `/bin/true`
 - `/usr/bin/passwd`
 - pueden existir usuarios sin acceso interactivo - ¿daemons?
- todos los usuarios tienen un directorio home para guardar sus datos y configuraciones
- root es un usuario especial sin limitaciones de acceso a recursos.
- los usuarios del sistema se pueden meter en uno o varios grupos
- los usuarios no son solo las personas que usan el sistema, también existen del sistema propiamente dicho, que nos permite aplicar restricciones o facilidades de acceso a recursos
- comandos asociados
 - `pwd` : da la ruta dónde estoy
 - `whoami` : indica cuál es mi usuario
 - `who` : usuarios que están conectados al sistema
 - `id` : indica quien soy, dándome el UID, GID y grupos adicionales
 - `useradd` → permite añadir un usuario
 - `$ useradd ciber3` → crea usuario con parámetros standard
 - en el `/etc/shadow` aparece con el símbolo `!` → hay que asignarle contraseña
 - hay que crear a mano el directorio y asignar permisos
 - `$ passwd <user>` : para cambiar la contraseña del usuario actual o, si eres **root**, el de cualquier usuario
 - `usermod` : modificar usuario
 - `userdel` : borrar usuario
 - `groupadd` : añadir un grupo al sistema
 - `groupdel` : borrar grupo de un sistema
 - `gpasswd` : cambiar password de un grupo
 - `su` : cambio de usuario «en caliente»
 - `newgrp` : cambia el grupo con el que hemos hecho login (pide contraseña de grupo)
- estructura fichero `/etc/passwd`
 - líneas, cada línea es un usuario del sistema
 - se puede editar el fichero para añadir, quitar y modificar
 - `nombre:password:user_id:group_id:nombre_administrativo:directorio_home:programa_interactivo`
 - `password`: antiguamente estaba el password encriptado, ahora suele haber una `X` que indica que el password está almacenado en `/etc/shadow`
 - `user_id`: ha de ser único
 - `group_id`: es el grupo principal, puede pertenecer a más
- estructura fichero `/etc/shadow`
 - `nombre:password:campossss:`
 - `password`: `*` indica que no es interactivo, `!` que no tiene contraseña, el resto es la contraseña
 - el resto de campos tiene que ver con la caducidad, preaviso, etc...
- estructura fichero `/etc/group`
 - `nombre:contraseña:group_id:usuario,usuario,usuario`
 - si el grupo no tiene usuario asignados (o ese grupo es el principal del usuario)
 - la contraseña se usa en conjunción con el comando `newgrp`

permisos de acceso a archivos

- se contemplan 3 niveles de acceso y 3 perfiles de acceso
- niveles de archivos:

- lectura: r → leer el archivo
- escritura: w → permite modificar
- ejecución: x → solo útil para «binarios»
- la ausencia de permisos se indica con «-»
- niveles de directorios:
 - lectura: r → mirar el contenido
 - escritura: w → permite crear, borrar
 - ejecución: x → acceso al directorio, pasar a través de él, acceder
 - si no tienes r podrás pasar a través, pero no ver el contenido
- perfiles:
 - usuario: soy el propietario del fichero/directorio
 - grupo: pertenezco al grupo del fichero/directorio
 - otros: no soy ni el usuario ni pertenezco a ningún grupo
- representación de permisos de acceso a un archivo
 - se codifican como una ristra de letras «rwx» de 3 en 3 para representar el usuario, grupo y otros respectivamente
 - chmod: modificación permisos archivos
 - permite uso formato numérico (donde r=4, w=2 y x=1)
 - permite uso formato «cadena» → «u+x»: asigna al usuario el permiso de ejecución, «g-w»: le quita al grupo del fichero el permiso de escritura
 - touch: toca un archivo, actualizando la fecha de acceso. Si no existe, crea un archivo a 0 bytes.
 - permisos especiales:
 - sticky bit:
 - directorio: impide que el usuario pueda borrar archivos aunque tenga permiso de escritura si no son los propietarios del directorio
 - fichero:
 - \$ chmod 1777 <fichero> → rwxrwxrwt
 - \$ chmod 1776 <fichero> → rwxrwxrWT

particiones de discos

- /dev/sdxy
 - x = disco
 - y = partición
- \$ df: discos disponibles, su estatus y características
- mount
- umount
- /etc/fstab: montaje de dispositivos

gestión remota

- configuración Red:
 - /etc/sysconfig/network/ifcfg-eth0
 - /etc/sysconfig/network/routes
 - /etc/resolv.conf
 - \$ service network {start|stop}
 - \$ ifup <dispositivo red>
 - \$ ifdown <dispositivo red>
 - ifconfig
 - netstat, netstat -i, netstat '' * '' netstat -tupln | grep :22: muestra programas escuchando, es este caso, puerto 22

From:

<https://matebcn.eu/> - **miguel angel torres egea**

Permanent link:

<https://matebcn.eu/info:cursos:cibernarium:linux1>

Last update: **26/09/2020 13:07**

