MANUAL DEL ADMINISTRADOR DE SISTEMAS GNU / LINUX

Índice:

TEMA 1: INTRODUCCIÓN A LOS SISTEMAS GNU / LINUX

MANUALES DE AYUDA:

- whatis <command> : Busca en su base de datos del manual del sistema una breve descripción del uso del comando.

- apropos <text> : Busca en la base de datos del manual del sistema las coincidencias con el texto especificado. Ya sea en el nombre o en la definición de un comando.

- man [<int>] <command>: Manual de comandos del sistema. Consulta el comando especificado así como una sección de este si es especificada. Las secciones se mueven el el rango [1-9] y cada una puede mostrar distinta información útil sobre el comando especificado.

  - Opciones:

    1. -k <command> → Equivale a usar el comando apropos.

  - Buscar en el manual:

    1. /<text> → Busca la cadena de texto introducida.

       n →Busca la siguiente coincidencia con la cadena de texto buscada.

       N → Navega a la coincidencia de texto anterior.

COMANDOS DE LINUX:

- time <command> : Cronometra la ejecución de un programa y indicando cuanto tardo este en ejecutarse.

- echo <text> : Muestra una cadena de texto por pantalla.
    - Opciones:
        1. -n → La palabra se imprime sin añadir el retorno de carro.
        2. -e → Habilita las secuencias de caracteres con un significado especial.
    - Funcionamiento:
        1. “text\ → Permite concatenar el texto de la linea actual con la siguiente. El comando finaliza con el cierre de las comillas dobles.
        2. “text → Igual que el anterior pero sin meter al final una linea en blanco. El comando finaliza con el cierre de las comillas dobles.
        3. “text” → Las comillas dobles permiten construir cadenas de texto en las que se pueden realizar sustituciones de valores.
        4. ‘text’ → Las comillas simples se utilizan para imprimir texto literalmente, es decir, no se realizan sustituciones.
        5. `command` → Las comillas ladeadas permiten redirigir el resultado de un comando, de forma que podemos pasar este a una variable de entorno o a otro comando como si fuera un argumento.
- history: Muestra el listado del historial de comandos.
    - Funcionamiento asociado:
        1. ! <int> → Ejecuta el comando del historial con el número especificado.
        2. !! → Ejecuta el último comando del historial de comandos.
        3. CTRL + “r” <text> → Busca en el historial de comandos uno relacionado con la palabra escrita.
- env: Muestra las variables del entorno actual.
    - Opciones:
        - -u <varName> → Deshace de definición de la variable de entorno.

- set : Muestra todas las variables y funciones definidas para el entorno actual.
    - Sintaxis:
        1. set
    - Variables de entorno más comunes:
        - $PWD → Contiene el directorio actual.
        - $HOME → Imprime el directorio home del usuario actual.
        - $? → Contiene la salida del último comando ejecutado.
        - $$ → Devuelve el Process IDentificator del proceso actual.
        - $PPID → Devuelve el Parent PID.
        - $PATH → Contiene los directorios de programas ejecutables.
        - $USER → Nombre de usuario.
        - $TERM → Tipo de terminal.
        - $SHELL → Terminal de comandos por defecto.
        - $PS1 → Contiene el prompt del usuario.
        - $HOSTNAME → Nombre de la máquina.
        - $RANDOM → Devuelve un número aleatorio.
        - EDITOR → Devuelve el editor de texto que se usa por defecto.
    - Crear nuestras propias variables de entorno:
        - varName=<int>
        - varName=”text”
        - varName=`command`
    - Imprimir el nombre de las variables de entorno:
        - echo “$varName”
        - echo “${varName}”
        - Es una buena práctica usar las llaves para imprimir el nombre de una variable, ya que algunas veces pueden darse confusiones de nombres.

- Cuando se lanza un conjunto de comandos como un único programa, el proceso actual crea un proceso hijo haciendo fork en el que se realiza la ejecución. Este proceso hijo no comparte las variables de entorno con el proceso padre, por tanto el padre ha de exportarlas, de esta forma las variables pueden ser vistas de forma global por los hijos:
    - export <varName>
    - export <varName>=<int>
    - export <varName>=”value”

- exit <int> : Termina el proceso actual inmediatamente, devolviendo como resultado de la ejecución el número especificado. Por defecto, en los sistemas GNU/LINUX cualquier número distinto de cero implica que la ejecución no se realizó correctamente.

- unset <varName> : Borra la variable de entorno especificada.

- ls <path> : Lista el contenido del directorio especificado.
  - Opciones:
    - -a → Muestra también los ficheros ocultos (.fileName).
    - -l → Ver las propiedades de los i-Nodos asociados a los ficheros.
    - -h → Mostrar el tamaño de los ficheros en Kb en lugar de Bytes.
    - -i → Mostrar el número del i-Nodo asociado.
    - -F → Mete un carácter al final de un nombre de fichero listado para indicar que tipo de fichero es.
      - / → Indica que es un directorio.
      - * → Indica que es un ejecutable.
      - @ → Enlaces simbólicos.
      - | → Pila FIFO.
      - y → Sockets.
    - -d →Informa solo sobre el directorio y no de sus contenidos.
    - -f → Imprime el contenido del directorio sin ordenar.
    - --color → Colorea la salida en función del tipo de fichero.
    - -1 → Imprime la salida en una sola columna.

- ps : Informa sobre los procesos activos.
    - Opciones:
        - [-]a : Lista todos los procesos de un terminal.
        - [-]u : Muestra la salida orientada al usuario.
        - [-]x : Muestra los procesos sin un terminal asociado.
        - -e : Selecciona todos los procesos.
        - -H : Muestra los procesos en formato de árbol.
        - -j : Formato de tareas.
        - -l : Formato largo.
        - -o : Permite especificar los campos que se desean visualizar.
        - -f : Muestra el listado con formato de arbol.
- sort <files> : Ordena alfanuméricamente el contenido de un fichero mediante una comparación byte a byte.
    - Opciones:
        - -n : Ordena numéricamente.
- which <command> : Devuelve las rutas completas de los ficheros a ejecutar para el comando pasado por parámetro.
- alias aliasName=’command commandOptions’ : Apoda un comando.
- unalias <varName> : Elimina un alias.
    - Opciones:
        - -a : Elimina todos los alias.
- cat <files> : Concatena uno o mas ficheros y los muestra por pantalla.
- head <file> -n <int> : Muestra las nº primeras líneas de un fichero.
- tail <file> -n <int> : Muestra las nº últimas líneas de un fichero.
- rm <files> : Borra uno o varios ficheros.
    - Opciones:
        - -r : Borra recursiva-mente un directorio.

- rmdir <directory> : Borra un directorio, pero no su contenido.
    - Opciones:
        - -p : Elimina todos los directorios padre que se queden vacíos como consecuencia del borrado.
- dmseg : Muestra todos los mensajes del kernel desde el último inicio.
- mkdir <dirName> : Crea un directorio con el nombre especificado.
    - Opciones:
        - -p <path> : Construye la ruta de directorios especificada.
- cd <path> : Cambie el directorio actual por el directorio especificado.
    - - : Si se utiliza el guión en lugar de una ruta, se va al directorio anterior, que no es necesariamente el directorio padre.
    - ~ : Si se utiliza en lugar de una ruta, el directorio actual es el directorio home del usuario actual.
- read <variables> : Lee una línea de la entrada estándar y asigna cada palabra a la variable correspondiente.
    - Opciones:
        - -d : Establece un delimitador para la lectura de la línea.
        - -n: Permite especificar el máximo número de bytes a leer.

- find <path> <conditions> : Busca en la ruta los ficheros con las características especificadas mediante las condiciones.
    - Conditions:
        - -name <fileName> : Busca en el path ficheros que tengan coincidencias con el nombre especificado.
        - -type <letter> :
            - b : Fichero especial de bloque.
            - c : Fichero especial de carácter.
            - d : Directorio.
            - p : Fifo o pila.
            - l : Enlace simbólico.
            - s : Socket.
            - f : Fichero plano.
        - -mtime <signed int> : Localiza los ficheros ficheros modificados por última vez hace...
            - +n: Más de de nº días.
            - -n: Menos de nº días.
            - n: nº días exactamente.
        - -exec <command> {} \; : Para los ficheros encontrados, estos son pasados al comando especificado. Donde {} sustituye al fichero actual y \; indica el carácter de escape.
- wc <file> : Contador.
    - Opciones:
        - -l : Cuenta las líneas de un fichero.
        - -b : Cuenta los bytes de un fichero.
        - -m : Cuenta los caracteres de un fichero.
        - -w : Cuenta las palabras de un fichero.
- tr [[set1] [set2]] “o” tr [“list1” “list2”] : Traductor de caracteres, sustituye unos por otros.
    - Opciones:
        - -d <list> : Borra los caracteres especificados.

- grep <text> <files> : Busca en uno o más ficheros las líneas que coinciden con un patrón de texto.

- cut <files> : Corta las columnas o campos de uno o más ficheros.

  - Opciones:

    - -b <int - int> : Especifica el rango de bytes a imprimir.
    - -c <int - int> : Corta las posiciones de columna especificadas en la lista.
    - -d <char> : Especifica el delimitador de campo, se usa con -f.
    - -f <int - int> : Corta los campos especificados en la lista.

- test <expression> : Evalua la expresión y devuelve 0 si es true.

- mv <origins> <destiny> : Mueve o renombra ficheros y directorios.

- cp <origins> <destiny> : Copia ficheros al lugar especificado.

  - Opciones:

    - -r : Permite copiar un directorio recursivamente.
    - -f: Elimina un fichero existente en el destino si este no se puede abrir.
    - -i: Pregunta antes de sobreescribir los ficheros de destino.

- zenity: Comando que llama a la API de GTK para poder hacer scripts con ventanas graficas.

- seq <int/int-int/first-increment-last> : Imprime el rango numérico especificado.

- date + “string format” : Imprime la fecha del sistema con el formato dado.

- sleep <int/s|m|h> : Espera una cantidad determinada de tiempo para continuar.

EDITOR DE FLUJOS SED:

- Sintaxis:
  - sed ‘commands’ <files>
- Uso de los comandos de sed:
  - ‘nº s/find/replace/g’ → Encuentra el texto especificado y lo sustituye por otro.
  - ‘ [nº] [n1,n2] [n1-nn] d’ → Elimina el número de línea especificada por el número o por los rangos numéricos.
- Caracteres especiales:
  - Un numero antes del comando indica a que linea de la entrada afecta el comando lanzado.
  - ? : Representa una coincidencia con cero uno caracteres precedentes.
  - El carácter “.” se emplea para especificar cualquier caracter.
  - El carácter “*” viene a significar cero o más coincidencias con el carácter anterior.
  - ^ : Coincide con el comienzo de una línea o cadena.
  - $: Coincide con el final de una línea o cadena.
  - Cada carácter “&” indica que el patrón a buscar se ha de poner tantas veces en la cadena final como “&” haya.
  - El carácter “g” detrás de la ultima contra-barra indica que el comando se aplica con todas las ocurrencias. Si no se especifica, sólo se buscará la primera ocurrencia de cada línea.
  - El carácter “i” detrás de la ultima contra-barra indica que no se hace distinción entre mayúsculas y minúsculas.

CARACTERES ESPECIALES Y FORMATOS DE COMANDOS:

- ~ : Representa el directorio home.
- . : Representa una coincidencia con cualquier carácter.
- * : Representa una coincidencia con cero o más caracteres.
- ? : Representa una coincidencia con cero uno caracteres.
- [ ]: Conjunto
  - [] Cualquier carácter contenido en el conjunto.
  - [!] Cualquier carácter no contenido en el conjunto.
  - [-] Cualquier carácter comprendido entre uno inicial y uno final.
  - [!-] Cualquier carácter menos los que se encuentran en el intervalo.
  - [^]Cualquier conjunto de caracteres que no contengan los especificados.
- ; Separador de comandos.
  - Sintaxis:
    1. cmd1 ; cmd2
- && AND, ejecuta el siguiente comando si el anterior fue exitoso.
  - Sintaxis:
    1. cmd1 && cmd2
- || OR, ejecuta cmd2 si falla la ejecucion de cmd1, de lo contrario ejecuta cmd1.
  - Sintaxis:
    1. cmd1 || cmd2
- ( ) Los paréntesis permiten agrupar un conjunto de comandos que son lanzados en un proceso de terminal hijo del proceso actual mediante forfk.
  - Sintaxis:
    - (cmd1 ; cmd2)

- $( ) Es una alternativa a `cmd`. Devuelve la salida de ejecutar todos los comandos del conjunto.
    - Sintaxis:
        - $(cmd ; cmd)
- {} Las llaves permiten agrupar un conjunto de comandos que son lanzados en el proceso de terminal actual.
    - Sintaxis:
        - { cmd1 ; cmd2 ; }
- | Canalización o ”Pipe”: Pasa la salida de un comando a la entrada de otro.
    - Sintaxis:
        1. cmd1 | cmd2
- ! <cmd> : Devuelve la negación al estado lógico de la salida del comando.

PROCESOS:

- Todo proceso tiene un Process Identificator (PID) que le es asociado.
- Todo proceso posee tres descriptores de fichero asociados (puede tener más):
  - 0 “o” stdin → Apunta al dispositivo de entrada, por defecto el teclado.
  - 1 “o” stdout → Apunta al dispositivo de salida, por defecto la pantalla.
  - 2 “o” stderr → Apunta al dispositivo mediante el cual se muestran los mensajes de error, por defecto es la pantalla.
- Redirección utilizando los descriptores de fichero:
  - cmd > file → Redirige la salida del comando a un fichero, sobreescribiéndolo si estfe ya existía.
  - cmd >> file → Redirige la salida del comando a un fichero añadiendo a este la información de salida por el final.
  - cmd < file → Utiliza el contenido de un fichero como entrada para el comando empleado.
  - cmd << text → Nos permite teclear todo el flujo que recibirá un comando, el final se indica cuando se teclea el texto especificado, entonces el flujo le es pasado al comando.
  - cmd 2> file →Envía los errores de ejecución del comando al fichero.
  - cmd > file 2>&1 → Envía las salidas de error y la salida normal al fichero.
  - cmd &> file → Añade el error estándar y la salida estándar al fichero.
  - cmd > f1 2> f2 → Envía la salida estándar a f1 y el error estándar a f2.

FICHEROS ESPECIALES:

/dev/null → Es un fichero al que redireccionar cualquier cosa innecesaria o que no necesitemos recuperar. Es algo así como la papelera.

/etc/shadow → Contiene las contraseñas de los usuarios cifradas.

/etc/passwd → Es un registro en el que están los usuarios del sistema.

ATAJOS DE LA CONSOLA BASH:

- *TAB: Permite completar una palabra que se ha comenzado a escribir en la terminal de comandos.*
- *ctrl + a : Posiciona el cursor al principio de la línea.*
- *Ctrl + e : Posiciona el cursor al final de la línea.*

BASH SCRIPTING:

Un script es un conjunto de ordenes del interfaz de comandos que están almacenados en un fichero y que se ejecutan de forma secuencial al ser llamado.

Para lanzar el script hay varias opciones:

- *./<fileName> [arguments] → Requiere permiso de ejecución sobre el fichero.*
- *bash <fileName> [arguments]*
- *sh <fileName> [arguments]*

Todos los ficheros de scripting comienzan con una línea que le indica al sistema con qué interprete de comandos se va a ejecutar el script:

#!/bin/bash → Indica que el script va a ejecutarse empleando el intérprete bash.

#!/bin/sh → Indica que el script va a ejecutarse empleando el intérprete sh.

En bash scripting [ ] es un sinónimo del comando test.

Los argumentos de un script son accedidos por su posición: $1, $2, $3 ...

$0 hace referencia al nombre del propio fichero que se está ejecutando.

$ hace referencia a todos los argumentos.*

$# hace referencia al número de argumentos.

Estructuras de control en bash script:

```
if [ condition ]
then
commands
elif [ condition ]
then
commands
else
commands
fi

for varName in list
do
commands
done

for varName in `seq <int>`
do
commands
done

for (( variable ; condition ; increment ))
do
commands
done

until [ condition ]
do
commands
done

while [ condition ]
do
commands
done

case varName in
pattern)
commands
;;
*)
commands
;;
esac
```

select varName [in list]
do
commands
done

Variables en bash script:

Las variables pueden almacenar cualquier tipo de datos. No existe un tipo de datos como tal.

- *Tipos de variables:*
  - *local <varName> : Variable de ámbito local.*
  - *<varName> : Variable de ámbito global.*

Funciones en bash script:

- *Declarar una función:*

  function <functionName>() {

  commands

  [return]

  }

- *Llamar a una función: <functionName> [arguments]*
- *Podemos usar una sentencia de retorno si queremos que la función devuelva como resultado un valor entero: return <int>*
- *Una función accede a los argumentos de la misma forma que un script.*

Operadores en bash script:

var=<int>
var=`expr $var + <int>` ↔ let var=var+<int> ↔ ((i = i + <int>))

var=<text>
var+=<text>

EL EDITOR DE TEXTO VI:

- *Comandos de trabajo:*
  - *Esc + u → Deshacer.*
  - *Esc + i → Insertar texto.*
  - *Esc + a → Añadir texto.*
  - *Esc + x → Suprimir carácter.*
  - *Esc + d + d → Borra la línea actual.*
  - *Esc + <int> + d → Cortar n.º líneas.*
  - *Esc + p → Pegar.*
  - *Esc + y +y → Copia la línea actual.*
  - *Esc + <int> + y → Copia n.º líneas.*
  - *Esc + O → Abre una nueva línea desplazando el texto de la línea actual.*
  - *Esc + o → Abre una nueva línea sin desplazar el texto de la línea actual.*
  - *Esc+/<word> → Busca la palabra especificada. ('n' Pasa a la siguiente).*
- *Comandos de guardado:*
  - *Esc + :q → Salir guardando los cambios.*
  - *Esc + :q! → Salir sin guardar los cambios.*
  - *Esc + :w → Guardar los cambios.*
  - *Esc + :w! → Sobre-escribir el fichero.*
  - *Esc + :wq → Guardar cambios y salir.*
  - *Esc + :wq! → Sobre-escribe el fichero y sale.*
- *Sustituciones de texto:*
  - *Esc + :%s/<find>/<replace>/<i/g/>*

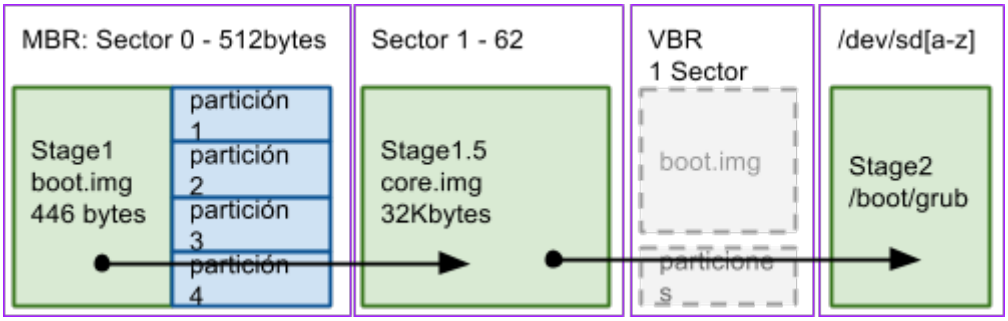
TEMA 2: INSTALACIÓN DEL SISTEMA OPERATIVO CentOS

ARRANQUE DEL SISTEMA OPERATIVO:

El arranque del sistema comprende desde el momento en que se pulsa el botón de encendido hasta que el sistema operativo ofrece la posibilidad de acceder a él (login).

La primera parte de este proceso que culmina cuando se cargado el kernel del sistema y este comienza con el arranque de los distintos servicios.

Actualmente existen dos estándares para la disposición de la información en el disco (particionado) y el proceso de arranque: BIOS (tradicional) y UEFI. Aunque UEFI pretende solucionar algunas de las limitaciones del esquema tradicional, este presenta algunos problemas (secure boot, firmware bugs, licencias, etc) por lo que BIOS no se ha abandonado completamente. Nosotros estudiaremos el estándar BIOS.



(Versión simplificada de la disposición del cargador en disco, particionado MS-DOS)

Pasos del arranque del sistema operativo:

1. Se carga el firmware, este “software” de tan bajo nivel se encuentra en una memoria ROM (Read Only Memory) de la placa base. Una vez cargado se ejecuta el BIOS (Basic Imput Output System), este lanzará el POST (Power On Self Test) para realizar comprobaciones sobre los componentes del sistema hardware.

2. La BIOS realiza la lectura y la carga del MBR (Master Boot Record), que es un registro de datos que se encuentra grabado en los primeros 512 bytes del sector 0 del disco duro. Este registro contiene la distribución de las particiones del disco. Con el estándar BIOS sólo puede haber un máximo de 4 particiones en el disco duro.

3. El BIOS carga y ejecuta GRUB, un software más potente para la carga de los sistemas operativos. Este se encuentra contenido a lo largo de los sectores 1 al 62.

4. Cuando GRUB carga, este se ocupará de realizar la lectura del resto de los sectores del disco para leer las particiones.

5. Una vez GRUB lee todo el disco, este muestra un menú interactivo que permite la carga en memoria del kernel de un sistema operativo así como de un RAM DISK.

6. Una vez elegido el kernel del sistema a cargar, se lanza el proceso init.

GERARQUÍA DE LOS SISTEMAS DE LOS SISTEMAS GNU/LINUX:

/bin	Contiene los comandos binarios básicos del sistema.
/boot	Contiene todo lo necesario para el proceso de arranque del sistema.
/dev	Contiene ficheros especiales de bloques y los ficheros asociados a dispositivos hardware.
/etc	Contiene los ficheros de configuración del sistema operativo y de las aplicaciones instaladas.
/home	Contiene todos los directorios de trabajo de los usuarios a excepción del root.
/usr	Contiene aplicaciones que son compartidas por todos los usuarios.
/usr/bin	Contiene los comandos binarios no administrativos, aquellos que pueden usar todos los usuarios.
/usr/include	Contiene todas las librerías del lenguaje C.
/var	Contiene archivos variables como logs, spool, bases de datos, e-mails y temporales. Datos susceptibles de cambiar durante la ejecución del sistema.
/var/log	Contiene los archivos de registro Log.
/var/lib	Contiene información a cerca del estado de los programas que se están ejecutando.

MÁQUINAS VIRTUALES:

- Definimos una máquina virtual como la descripción de un conjunto de hardware para poder simular un comportamiento mediante software.

- Virtual Box permite dos tipos de clonación de las máquinas virtuales:

  - Clonación completa: Se crea un duplicado total de un sistema escogido, el sistema original y el resultante son completamente independientes.

  - Clonación enlazada:

    - Se crea una instantánea de la máquina original que sirve de base para el nuevo sistema. El sistema clon es dependiente del sistema principal, ya que si a este le sucede algo el sistema clonado dejará de funcionar.

    - Las instantáneas son una forma de guardar el estado de la máquina virtual en un momento determinado, a partir del cual todo cambio que se haga en ella será almacenado en un nuevo archivo (*.vdi), manteniendo los originales intactos.

    - No podremos eliminar ninguna máquina virtual que tenga clonaciones asociadas a esta. Primero se han de eliminar las clonaciones y luego la máquina virtual original.

GRUB, LA SHELL DE ARRANQUE:

El menú de GRUB nos permite seleccionar el sistema operativo que queremos cargar, pero también proporciona otras opciones:

- “e” (edit): Permite editar el conjunto de comandos que se van a ejecutar cuando se selecciona una opción del menú de arranque de GRUB.
    - Los cambios realizados con esta opción sólo duraran lo que dure la sesión.
    - La opción (Ctrl + x) ejecutará el conjunto de comandos.
    - Instrucciones del GRUB:
        - set root=’hd0,msdos1’ (hd0,0): Este comando indica que el disco duro 0 va a ser el disco duro primario y que de este disco se procederá al montaje de la primera partición del disco.
        - insmod <FileName> : Carga un módulo del kernel.
        - linux16 (kernel): Carga una imagen del kernel de linux. Cualquier texto que le siga al fichero donde está el kernel, le es pasado a este como un lote de comandos a ejecutar.
            - \vmlinuz: Es un archivo ejecutable que contiene el kernel de Linux.
            - root=UUID=… : Identificador universalmente único., es un número que identifica de forma exclusiva una partición del disco.
            - ro: Monta el sistema de fichero raíz con permisos de solo lectura.
            - rhgb: Red-Hat Graphical Boot. Modo de arranque gráfico.
            - quiet: Modo silencioso, suprime la mayoría de los mensajes del modo de arranque gráfico.
            - LANG=en_US.UTF-8 → Especifica la codificación de caracteres.
            - single: Inicia Linux en modo mono-usuario. Esta opción se usa para la administración y recuperación del sistema. Proporciona un prompt raíz en cuanto se inicia el sistema, con una inicialización mínima, no se permiten otros accesos.
            - init=<file>: Indica el nombre del primer proceso que se ha de ejecutar tras la carga del kernel.

- systemd.unit=<unit>.target : Permite seleccionar el nivel de ejecución con el que ha de arrancar el sistema operativo. Por ejemplo systemd.unit=emergency.target hace que se arranque el sistema en el modo seguro, que es equivalente al modo monousuario.

  - initrd16 (initrd): Proporciona un proceso de arranque en dos etapas. Primero configura un sistema de ficheros raíz temporal en un disco RAM que contenga los módulos que se necesitan añadir al kernel, luego los carga y montar el sistema de ficheros real. El RAM DISK que contiene el sistema de ficheros temporal es el fichero de dispositivo especial "/*dev*/initrd".

- "c" (command): Permite acceder a una interfaz de comandos para ejecutarlos de forma manual.

GRUB, FICHEROS DE CONFIGURACIÓN:

- Cada vez que se instala un nuevo sistema operativo el fichero de configuración de GRUB es devuelto a su estado inicial, a menos que los cambios los realicemos desde otros ficheros que definen como ha de generarse este.

- El fichero de configuración de GRUB es: /*boot*/grub2/grub.cfg

- Los valores por defecto de las variables del cargador GRUB se encuentran en el fichero: /etc/default/grub

  - En caso de modificar este fichero, hay que actualizar el fichero grub.cgf, esto puede hacerse mediante el comando grub2-mkconfig.

  - grub2-mkconfig -o /boot/grub2/grub.cfg: Actualiza el fichero de configuración /etc/default/grub teniendo en cuenta los valores por defecto de GRUB en /etc/default/grub y otros scripts de /etc/grub.d/

    - /boot/grub2/grub.cfg → Fichero en el que se encuentra la configuración final de GRUB. Esta se monta teniendo en cuenta los siguientes ficheros:

      - /etc/default/grub → Aqui se definen el valor que toman por defecto algunas de las variables de GRUB.

        - GRUB_TIMEOUT → Marca el número de segundos que GRUB esperará a elegir una opción de arranque antes de cargar el sistema de forma automática. Con -1, el tiempo de espera es indefinido.

- scripts de /etc/grub.d/ :
    - 01_users: Permite especificar claves para el arranque de un kernel de linux o para acceder a los menús de edición o al menú de comandos de GRUB.
        - set superusers=”userName” : Especificamos el nombre del usuario administrador.
        - password <userName> <password> : Si queremos especificar la contraseña en texto plano.
        - grub2-mkpasswd-pbkdf2 : Genera una contraseña encriptada.
        - password_pbkdf2 <userName> <encryptedPassword> : Si la queremos especificar encriptada.
    - 10_linux: Si quitamos de la variable CLASS la opción que pone el --unrestringed, entonces también pide una contraseña para cargar el kernel seleccionado en el menú de GRUB.

LAS HERRAMIENTAS SYSTEMD:

- systemd: Conjunto de demonios, bibliotecas y herramientas diseñadas para realizar tareas de administración del sistema. Permiten interactuar de forma sencilla con el núcleo del sistema operativo.
- Estas herramientas se encuentran ubicadas en /systemd
- Systemd trabaja con una serie de elementos o unidades:
    - target: Servicios de ejecución a activar (Conjunto de services).
    - service: Programas.
    - timer: Temporizador para la ejecución programada de tareas.
    - mount: Punto de montaje para un sistema de ficheros.
    - path: Permite activar una unidad de tipo service especificando su ruta.

- La herramienta systemctl:
  - Opciones:
    - list-unit-files → Muestra el estado de todas las unidades del sistema.
      - enabled: Son aquellos servicios que se cargan durante el arranque.
      - static: Servicios que dependen de otros servicios para ser ejecutados.
      - disabled: Son aquellos servicios que no han de cargarse durante el arranque del sistema.
    - list-units: Lista las unidades activas.
      - loaded: systemd ha cargado el archivo.
      - active: Error / Ok.
      - sub: Sub estado.
    - status: Da información mas detallada de las unidades.
    - is-enabled <ServiceName> : Indica si esta habilitado un servicio.
    - is-active <ServiceName> : Indica si el servicio se está ejecutando.
    - start [--now] <ServiceName> : Ejecuta un servicio no.
    - stop [--now] <ServiceName> : Detiene un servicio.
    - restart [--now] <ServiceName> : Reinicia un servicio.
    - enable [--now] <ServiceName> : Habilita un servicio. El servicio es cargado durante el arranque del sistema operativo.
    - disable [--now] <ServiceName> : Indica al sistema que el servicio no ha de cargarse automáticamente durante el arranque.
    - mask [--now] <ServiceName> : En este estado, un servicio no puede ejecutarse automáticamente o manualmente.

      NOTA: --now es necesario si queremos que la orden tenga efecto inmediato, si no se especifica, entonces tendrá efecto durante la próxima carga del sistema operativo.

- get-default: Devuelve el nivel de ejecución que por defecto es graphical.
- set-default <Level> : Cambia el nivel de ejecución por defecto.
- isolate <Level> : Cambia el nivel de ejecución actual.
    - Levels:
        - poweroff.target: Apagado completo del sistema.
        - rescue.target: Modo de recuperación, ejecuta una consola de mantenimiento.
        - multi-user.target: Entorno multi usuario sin escritorio gráfico.
        - graphical.target: Entorno multi-usuario con escritorio.
        - reboot.target: Apagado y reinicio del sistema.
- reboot: Reinicia la máquina.
- poweroff: Apaga correctamente la máquina.

- Espcificadores de opciones:
    - --type=<unit list> : El argumento debe ser una lista separada por comas o una unidad en concreto, como por ejemplo service o socket.

OTRAS HERRAMIENTAS:

- dd: Hace una copia de un fichero de entrada (if/InputFile) y envía los resultados a un fichero de salida (of/OutputFile). Esta herramienta manipula ficheros a nivel de bit.
    - Opciones:
        - bs=<int>{B,K,M,G} → Establece el tamaño de bloque para la entrada (ibs) y la salida (obs).
        - count=N → Copia sólo N bloques de entrada en la salida.
        - if=<FileName> → Especifica el fichero de entrada.
        - of=<FileName> → Especifica el fichero de salida.
        - seek=N → Se salta los primeros N bloques del fichero de salida.
        - skip=N → Se salta los primeros N bloques del fichero de entrada.
- fdisk: Comando que muestra información sobre las particiones de un disco.
    - Opciones:
        - -l : Lista las tablas de partición y finaliza.

TEMA 3: GESTIÓN DE APLICACIONES Y ACTUALIZACIONES

Tipos de distribución (Release):

- Rolling: Distribuciones de actualización contínua.
- Patrones de mantenimiento:
  - STL (Long Term Support): Distribuciones que se comprometen a ser mantenidas a lo largo del tiempo.

Gestión de software:

- Paquete: Conjunto formado por varios software y metadatos asociados a estos.
  - Elementos de un paquete:
    - Archivos: Ficheros reales que componen el paquete.
    - La cabecera: Contiene toda la información sobre el paquete (nombre, versión, descripción, ficheros, copyright y localización del fichero fuente).
    - La firma: Contiene información para verificar la integridad y la autenticidad del paquete.
- Dependencias: Son aquellos otros paquetes de los que un paquete concreto necesita para poder funcionar.
- Repositorio: Servidor que contiene paquetes de software, es posible conectarse a él mediante protocolos como http o ftp.
- Mirror: Son aquellos servidores que ofrecen los mismos paquetes que puede ofrecer un repositorio, el objetivo de estos es poder acceder a los mismos paquetes de un repositorio a través de distintos servidores.

- Programas para la gestión del software:
    - Debian, Ubuntu y Mint: dpkg y apt-get.
    - RedHat y Fedora: rpm y yum.
    - Arch y Manjaro: pacman.

Las herramientas rpm y yum:

- rpm (Redhat Package Manager): Es el administrador de paquetes de RedHat, permite realizar varias funciones como crear, instalar, consultar, etc.
    - Opciones:
        - -i <Package> : Instala el paquete especificado.
            - -v : Detallado, imprime los mensajes de progreso.
            - -h : Imprime hasta 50 marcas hash mientras se desempaqueta el archivo del paquete.
            - --force : Fuerza la instalación del paquete.
        - -e <Package> : Elimina el paquete especificado.
        - -U <Package> : Actualiza el paquete especificado, si no está instalado lo instala, de forma que actúa como -i.
        - -q <Query Options> <Package> : Permite consultar paquetes existentes, ofreciéndonos alguna información sobre ellos (nombre-versión-release-arquitectura).
            - -a : Consulta todos los paquetes instalados.
            - -f <fileName> : Imprime el paquete de software relacionado con el fichero especificado.
            - -i : Muestra la información del paquete (Nombre, versión, descripción, etc).
            - -l : Lista todos los ficheros del paquete.

        - -V <Package> : Compara la información de un paquete instalado con la información del paquete original. La información comparada incluye: El tamaño del fichero, el tipo del fichero, el propietario, el grupo, la última modificación, etc. En conclusión, nos dice si un paquete ha sido modificado en algún aspecto.

- yum (Yellowdog Updater Modified): Programa que permite realizar tareas de administración de paquetes (*.rpm) de una forma más automatizada. Incluye entre otras cosas: La instalación, actualización, eliminación y mantenimiento de paquetes de sotware.

    - Ficheros asociados:

        - El fichero de configuración de yum es: /etc/yum.conf

        - Localización de los archivos de los repositorios: /etc/yum.repos.d

            - Características de los ficheros (*.repo):

                - name → Nombre del repositorio.

                - mirrorlist → Una lista de mirrors desde la cual yum selecciona el más próximo geográficamente.

                - baseurl → Si se usa en lugar de mirrorlist, indica un repositorio fijo.

                - gpgcheck → Indica si se necesita una clave pública para usar el repositorio.

                - gpgkey → La ruta al archivo de la clave pública.

                - enabled → Desabilita el repositorio.

    - Opciones:

        - clean all : Borra todos los paquetes de la base de datos de yum.

        - update <Package> : Actualiza el paquete especificado, si no se especifica ninguno, se actualizarán todos los paquetes del sistema.

        - info <Package> : Muestra información de los paquetes especificados.

        - install <Package> : Instala el paquete de software especificado.

- remove <Package> / erase <Package> : Elimina el paquete especificado. Y todos los paquetes que son dependientes de este.

- list <TextPattern> : Muestra una lista de todos los paquetes que están instalados o listos para la instalación. Se puede usar un patrón de texto.

- list installed <TextPattern> : Muestra una lista de todos los paquetes que están instalados. Se puede usar un patrón de texto.

- search <Text> / search all <Text> : Localiza paquetes de software que coincidan con la cadena especificada, ya sea por una coincidencia en el nombre del paquete, la descripción, el resumen, el empaquetador, etc.

- grouplist : Muestra todos los grupos de software instalados.

- groupinfo <GroupName> : Muestra información sobre un grupo de paquetes de software.

- groupinstall <GroupName> : Instala un grupo de paquetes de software.

- repolist : Muestra una lista de los repositorios configurados y activos. Refresca la configuración de los ficheros de /etc/yum.repos.d

- list updates: Muestra una lista de todos los paquetes de software que necesitan ser actualizados.

Otros comandos:

- curl: Comando que puede transferir archivos desde un servidor a nuestra máquina o desde nuestra máquina a un servidor.
  - Opciones:
    - -O <URL> : Copia un fichero remoto y la guarda en nuestra máquina.
- mount: Muestra cuales son los directorios asociados a dispositivos hardware.
- touch <FileName> : Actualiza el último acceso que se realizó sobre el fichero al tiempo actual.
- chmod <OctalMode> <FileName> : Asigna los permisos de lectura, escritura y ejecución especificados a un fichero.
- less: Permite paginar una salida por pantalla, es una versión mejorada de more.

TEMA 4: ADMINISTRACIÓN DE USUARIOS Y GRUPOS

Comandos para la administración de usuarios y grupos:

- id : Muestra el id del usuario y de su grupo.
  - Opciones:
    - -u : Solo se muestra el uid.
    - -g : Solo se muestra el guid.
    - -G : Imprime sólo los grupos suplementarios.
    - -n [-u / -g] : Muestra el nombre de usuario o grupo.
- whoami : Impime el nombre del usuario actual, equivale a id -nu.
- w : Muestra los usuarios que han hecho login en el sistema y tienen un proceso de terminal asociado.
- su [<command>] : Por defecto crea un proceso de consola que se ejecuta bajo el id del usuario especificado. Si no se especifica ningún id de usuario, se crea un proceso de consola bajo el id de root. Si se especifica un comando y un usuario cuya contraseña es conocida, entonces se ejecutará el comando especificado bajo la entidad del usuario del que conocemos la contraseña.
  - Opciones:
    - : Sin parámetros, cambiamos a root.
    - - : Realiza la secuencia de login al completo, cambiando completamente al entorno del usuario root.
    - -l <UserName> : Realiza la secuencia de login al completo, cambiando completamente al entorno del usuario especificado.
    - -c “<Command>” : Ejecuta el comando en una nueva consola y finaliza.

- sudo [<command>] : Mecanismo que comprueba si un usuario tiene definidos los permisos de administrador para hacer uso de servicios, programas, comandos, etc.
    - Opciones:
        - -u : Permite ejecutar el comando como el usuario especificado.
        - -i : Realiza la secuencia de login al completo, cambiando completamente al entorno del usuario especificado.
- ls -l [<FileName>] : Toda la información posible del fichero.
    - El primer bloque de letras:
        - La primera letra de este bloque indica el tipo de fichero:
            - d → Directorio.
            - - → Fichero.
            - p → Pipe.
            - s → Socket.
            - c, b → Fichero de dispositivo.
            - l → Enlace.
        - Tipos de permisos:
            - r : Permiso de lectura. (Si aparece, indica bit de lectura activo).
            - w : Permiso de escritura. (Si aparece, indica bit de escritura activo).
            - x : Permiso de ejecución. (Si aparece, indica bit de ejecución activo).
        - Las tres siguientes letras indican los permisos que posee el usuario propietario. Cada letra representa el estado de un bit.
        - Las tres siguientes letras indican los permisos que poseen los usuarios que están en el mismo grupo que el propietario. Cada letra representa el estado de un bit.
        - Las tres siguientes letras indican los permisos que poseen otros usuarios. Cada letra representa el estado de un bit.

- Bits especiales:
  - setuid (s) :
    1. El suid bit es asignable a ficheros que pueden ejecutarse.
    2. Permite que cuando un usuario ejecuta un fichero con este bit activo, el proceso se ejecuta con los mismos permisos de el usuario propietario.
    3. Ejemplos de ficheros con este bit: El programa su. Este tiene que tener este bit activo para que cualquier usuario pueda adquirir temporalmente permisos administrativos para cambiar de usuario.
  - setguid (s) :
    1. Hace lo mismo que el setuid bit, pero con los permisos del grupo asignado al fichero.
    2. Cuando se aplica sobre un directorio, se obliga a que todos los archivos y directorios creados en ellos pertenezcan al grupo del dueño del directorio.
  - sticky (t) :
    1. El sitcky bit es un permiso de acceso a ficheros.
    2. Si se le aplica a un fichero, este solo puede ser modificado o borrado por el propietario del elemento o root. Aunque el resto de usuarios poseyera el permiso de escritura.
    3. Si se le aplica a un directorio significa que los elementos de este solo pueden ser modificados o borrados por el propietario del elemento, el propietario del directorio o root. Aunque el resto de usuarios poseyera el permiso de escritura.
    4. Ejemplos de ficheros con este bit: /tmp

- Número de enlaces al fichero.
- Nombre del propietario del fichero.
- Nombre del grupo propietario del fichero.
- Fecha de la última modificación del fichero.

- chmod <Permission> <Files> : Cambia los permisos de uno o más ficheros. Sólo puede cambiar los permisos de un fichero su propietario o root.
    - Formas de establecer los permisos:
        - Simbólica: <Target><Modifier><Type>,<Target><Modifier><Type> …
            - Objetivo de los permisos:
                1. u → Usuario propietario.
                2. g → Usuarios que pertenecen al mismo grupo del propietario.
                3. o → Otros usuarios.
                4. a → Todos (por defecto).
            - Modificador:
                1. + → Indica que se conceden permisos.
                2. - → Indica que se eliminan permisos.
                3. = → Asigna los permisos especificados denegando los demás.
            - Tipo de permisos:
                1. r → Permiso de lectura.
                2. w → Permiso de escritura.
                3. x → Permiso de ejecución (ejecutable) o permiso de acceso (dir).
                4. t → Sticky bit, se utiliza sobre todo en los directorios para evitar que otros usuarios no propietarios puedan modificar o borrar los ficheros que hay en el.
                5. s → setuid bit o setguid bit, permite ejecutar un fichero con los permisos del usuario propietario.
        - Octal: Se especifican tres números comprendidos entre el 0 y el 7. Los permisos se activan en función de su representación binaria. El orden es: Usuarios, grupo y otros usuarios. (Por defecto 775 al crearse un fichero)
            - Estos tres números pueden ser precedidos de un cuarto número:
                - 4 → Activa el setuid bit.
                - 2 → Activa el setguid bit.
                - 1 → Activa el sticky bit.
    - Opciones:
        - -R : Asigna recursiva-mente los permisos especificados a un directorio y a todos sus contenidos.

- umask <Mask> : Permite establecer los permisos por defecto cuando se crea un fichero. Los permisos finales se obtienen mediante la diferencia entre 777 y la máscara que se especifica. Cabe a decir que la máscara es una propiedad del proceso en ejecución (en este caso lo que dure el proceso de nuestra consola).
    - Opciones:
        - : Si no se especifica ninguna máscara, se puede consultar cual es la máscara actual.
- chown [<Propietary> / <Propietary:GroupPropietary>] <Files> : Permite cambiar el propietario de un fichero.
    - Opciones:
        - -R : Si se le aplica a un directorio, se cambia al propietario de todo su contenido de forma recursiva.
- chgrp <GroupPropietary> <Files> : Permite cambiar el grupo de usuarios al que pertenecen los ficheros.
    - Opciones:
        - -R : Si se le aplica a un directorio, se cambia el grupo propietario de todo su contenido de forma recursiva.
- uniq : Comando que recibe un flujo de entrada y elimina las líneas repetidas.
    - Opciones:
        - -d : Imprime solo las líneas duplicadas.
        - -u : Imprime solo las líneas únicas.
- sort -u : Primero ordena las líneas de un flujo de datos y luego elimina las líneas que están repetidas.
- vipw : Hace que eleditor de texto por defecto abra el fichero /etc/passwd.
- vigr : Hace que el editor de texto por defecto abra el fichero /etc/group.
- visudo : Permite editar el fichero /etc/sudoers.
- newgrp <GroupName> : Lanza un proceso de shell en el que el grupo principal del usuario es el nuevo grupo especificado.

- useradd <UserName> : Comando que permite crear cuentas de usuarios.
    - Opciones:
        - -c : Comentario sobre la cuenta.
        - -e : Fecha de expiración de la cuenta.
        - -f : Número de días que han de pasar para desactivar permanentemente la cuenta una vez expiró esta.
        - -g : Grupo principal al que pertenece el usuario.
        - -G : Grupos adicionales a los que pertenece el usuario.
        - -m : Crea el directorio home del usuario si este no existe.
        - -s : Define la consola de acceso para este usuario.
        - -d : Permite especificar el directorio home.
        - -p : Permite especificar la contraseña del usuario (encriptada).
- passwd <UserName> : Comando para cambiar la contraseña de un usuario.
- groupadd <GroupName> : Comando para la creación de nuevos grupos.
    - Opciones:
        - -g : Permite especificar el GID del grupo.
        - -p : Permite especificar una contraseña (encriptada) para el grupo.

- usermod <UserName> : Comando para modificar cuentas de usuario.
    - Opciones:
        - -g : Especifica el GID del grupo al que pertenece el usuario.
        - -G : Especifica los grupos secundarios, eliminando los antiguos.
        - -a : Se usa con -G, conserva los grupos secundarios actuales y añade los nuevos grupos especificados.
        - -s : Establece el proceso de shell asociado al usuario.
        - -u : Define el UID del usuario.
        - -g : Define el GID del usuario.
        - -L : Permite bloquear la contraseña de un usuario añadiendo ! delante.
        - -U : Desbloquea la contraseña de un usuario.
        - -p : Permite definir la contraseña (encriptada).

El fichero /etc/securetty:

Este fichero contiene todas las terminales desde las que se permite acceder a root.

El fichero /etc/security/access.conf:

Configura que usuarios y desde que terminales pueden entrar al sistema.

El fichero de usuarios /etc/passwd:

El contenido de este fichero determina quien puede acceder al sistema (login) de forma legítima.

Contenido del fichero (cat /etc/passwd | grep cursoasr):

cursoasr:x:1000:1000:cursoasr:/home/cursoasr:/bin/bash

1. Nombre de la cuenta de usuario.
2. Clave de acceso encriptada.
3. UID de la cuenta.
4. GID del grupo al que pertenece la cuenta.
5. Nombre del usuario.
6. Directorio home del usuario.
7. Proceso shell asociado al usuario.

El fichero /etc/login.defs:

Contiene la configuración y valores por defecto para el mecanismo shadow.

En este fichero se definen:

- PASS_MAX_DAYS → Numero máximo de días que una contraseña puede ser usada.
- PASS_MIN_DAYS → Días que tienen que pasar para poder cambiar la contraseña.
- UID_MIN y UID_MAX → Definen el rango disponible de identificadores de usuario.
- GID_MIN y GID_MAX → Definen el rango disponible para los grupos de usuario.
- FAIL_DELAY → Tiempo que ha de pasar desde que fallamos al hacer login hasta que disponemos de un nuevo intento para identificarnos.
- LOGIN_RETRIES → Número máximo de intentos de que se dispone para hacer login.

El fichero de contraseñas /etc/shadow:

Este fichero almacena las contraseñas de usuario cifradas y nos da información sobre su caducidad y validez de la cuenta.

Contenido del fichero (cat /etc/shadow | grep cursoasr):

cursoasr
6ngf4FyexzROWo8HY$y0qXQv3gjhD22kNs8DyqDm3DaFW9SFDJJBj41MraKfUgQU/dlylA116Nr3emYz7cQu9A8D5QNbRgYfE5G.2cp/::0:99999:7:::

1. Nombre del usuario.
2. Contraseña cifrada.
3. Número de días desde que la contraseña fue cambiada por última vez.
4. Mínimo número de días para cambiar de contraseña.
    - :: → Sin contraseña.
    - :*: → Nunca tuvo una contraseña.
    - :!!: “o” :!: → Cuenta bloqueada. (Existe pero se considera que no se le ha dado una contraseña).
5. Número máximo de días de validez de la cuenta.
6. Días que debe avisarse al usuario antes de que caduque la contraseña.
7. Días para deshabilitar la cuenta después de que su contraseña caduque.
8. Fecha de caducidad, si se cumple la cuenta es deshabilita.

El fichero de grupos /etc/group:

En este fichero se encuentran definidos todos los grupos de usuarios del sistema.

El fichero de contraseñas de grupos /etc/gshadow:

Este fichero permite establecer una contraseña a un grupo de usuarios para evitar que cualquier usuario pueda unirse a un grupo concreto.

SUDO vs SU, eliminando brechas de seguridad:

- su → Permite ejecutar comandos como otros usuarios, lo que implica que tengamos que conocer previamente su contraseña.
    - Este comando supone una brecha de seguridad ya que no es lo más recomendable que los usuarios hayan de conocer las contraseñas de otros.
    - Por lo general es una mala práctica y se desaconseja su uso.
    - Lo más recomendable es desactivar la cuenta de root.
- sudo → Permite establecer un sistema de permisos para la ejecución de programas.
    - A diferencia de su es un mecanismo seguro, ya que solo recurre a la contraseña del usuario que lo utiliza, no requiere conocer otras contraseñas agenas al usuario actual.

Fichero /etc/sudoers:

- Contiene definido un sistema de permisos para la ejecución de programas.
- % → Indica grupos de usuarios.
    - %wheel → Este grupo está asociado a los administradores del sistema, estos usuarios pueden hacer uso de su y configurar sudo.
- Sintaxis: usuario máquina=(identidades de ejecución) comandos
    - Usuario.
    - Máquina: Especifica una máquina física.
    - Identidades de ejecución: Especifica como qué usuario se pueden lanzar los distintos comandos. (Usuarios:Grupos) Si se especifica ALL en ambos, significa que podemos lanzar comandos en nombre de cualquier usuario y también de cualquier grupo.
    - Comandos → Si se especifica NOPASSWD: <commandList/ALL>, no hace falta introducir la contraseña del usuario al lanzar los comandos.

Los ficheros de las cuentas de usuario /etc/skel:

Estos ficheros contienen la configuración global de:

- $HOME/.bashrc : Este fichero se ejecuta cada vez que cargamos una shell.
- $HOME/.bash_profile : Este fichero se ejecuta cuando se hace login correctamente.
- $HOME/.bash_logout : Este fichero se ejecuta al cerrar una sesión de usuario.

Los ficheros /etc/profile y /etc/profile.d:

Estos ficheros contienen la configuración global del entorno.

TEMA 5: ADMINISTRACIÓN SISTEMAS DE FICHEROS

Comandos para consultar el estado del sistema:

- lsblk : Lista los dispositivos de bloques y las particiones que tienen.
  - Si al listar los dispositivos aparece una estructura arbórea, esta es para mostrar las particiones.
  - Letras del dispositivo:
    - s (SATA) , h (IDE)
    - Identificador del dispositivo → Major number.
    - Identificador dentro del tipo → Minor number.
  - Opciones:
    - -h : Muestra un breve resumen de todas las opciones y los campos.
    - -I <majorNumber> : Solo muestra un tipo concreto de dispositivo.
    - -f : Muestra NAME, FSTYPE, LABEL, UUID, MOUNTPOINT.
    - -o <fieldList> : Permite especificar una lista de campos a mostrar.
      - Campos: NAME,MAJ:MIN,TYPE,FSTYPE,SIZE,MOUNTPOINT.
  - NOTA: En el primer bloque de un dispositivo de bloques hay una copia del MBR, en el segundo está la información del súper-bloque, el cual contiene información el sistema de ficheros de una partición. Este esquema se utiliza si elegimos que la tabla de particiones es del tipo ms-dos.
- du <file> : Devuelve el tamaño que ocupa un fichero.
  - Opciones:
    - -b : El tamaño se muestra en bytes.
    - -h : El tamaño se muestra en formato humano (KB, MB, GB, etc …).

- df : Informa sobre la cantidad de espacio libre de todos los sistemas de ficheros montados o en uno especificado.
    - Opciones:
        - -a : Muestra también todos los pseudo sistemas de ficheros.
        - -h : Imprime los tamaños en formato humano.
        - -m : Imprime los tamaños en megabytes.
        - -k : Imprime los tamaños en kilobytes.
        - -t <filesistemType> : Imprime los datos del tipo especificado.
        - -T : Muestra una columna con el tipo de sistema de ficheros.
        - -x <filesistemType> : Excluye los datos de los del tipo especificado.
- free : Muestra estadísticas sobre el uso de la memoria (libre, utilizada, física, de intercambio, compartida y los buffers del kernel) de todo el sistema.
    - Opciones:
        - -k : Muestra los tamaños en kilobytes.
        - -m : Muestra los tamaños en megabytes.
        - -g : Muestra los tamaños en gigabytes.
        - -h : Muestra la información en formato humano.
- mount <direcctory> : Sirve para montar un sistema de ficheros en un punto del árbol de directorios del sistema. Cuando se ejecuta sin argumentos muestra los sistemas de ficheros montados (tipo, dispositivo, opciones y punto de montaje).
    - Opciones:
        - -a : Remonta todos los dispositivos especificados en /etc/fstab
        - -t <fileSystemName> : Solo muestra los datos del sistema de ficheros que se especifica. Esta opción también permite montar un sistema de ficheros del tipo especificado.
- umount <directory> : Desmonta el sistema de ficheros especificado.

Comandos generales de particionado:

- fdisk <partitionName> : Este comando por defecto muestra la información sobre las particiones del disco. También puede crearlas y borrarlas, así como indicar cual es la partición activa. Posee un menú interactivo para trabajar con el dispositivo o participación especificada.
    - Opciones:

        - -l : Lista las tablas de partición y finaliza.

    - Opciones comunes del menú interactivo:

        - d → Elimina una partición.
        - l → Muestra una lista con los tipos conocidos de partición.
        - m → Volver a imprimir el menú interactivo.
        - n → Crea una nueva partición.
        - o → Crea una nueva tabla de particiones vacía de tipo DOS.
        - p → Imprime la tabla de particiones del dispositivo.
        - q → Sale del programa sin guardar los cambios.
        - t → Permite especificar los sistema de ficheros en la tabla de particiones.
        - v → Comprueba el estado de la tabla de particiones.
        - w → Escribe los cambios en el disco y sale del programa.

Comandos para particiones de intercambio:

- mkswap <partitionName> : Permite establecer el espacio de intercambio en el la partición especificada del dispositivo. También puede hacerse en un fichero.

- swapon <partitionName> : Hace que los dispositivos especificados estén disponibles para intercambio y paginación.

    - Opciones:

        - -s : Imprime las particiones de intercambio y datos de su uso.

- swapoff <partitionName> : Hace que los dispositivos especificados dejen de estar disponibles para intercambio y paginación.

Comandos para el uso y mantenimiento de sistemas de ficheros:

- mkfs <partitionName> : Construye un sistema de ficheros en una partición.

    - Opciones:

        - -t <type> : Permite especificar el tipo de sistema de ficheros a construir

- tune2fs <partitionName> : Permite ajustar los parámetros de un segundo sistema de ficheros extendido de Linux ajustando varios parámetros.

    - Opciones:

        - -l : Consulta las características del sistema de ficheros especificado.

        - -L <label> : Permite establecer una etiqueta a un sistema de ficheros.
        - -j : Crea un registro (journaling), permite pasar de ext2 a ext3.
- blkid : Devuelve los identificadores de las particiones (UUID : Universal Unique IDentifier) y los tipos de partición.
- dumpe2fs <deviceName> : Imprime información del superbloque y el grupo de bloques del dispositivo.
- fsck <fileSystemName> : Permite comprobar y reparar sistemas de ficheros.
- e2fsck <fileSystemName> : Hace exactamente lo mismo que fsck pero este comando está más pensado para sistemas de ficheros ext2 y ext3 con un registro de journaling.
- resize2fs <partition> : Comando para re-dimensionar particiones de tipo ext.

Gestión de volúmenes lógicos (LVM)

LVM añade una capa de abstracción por encima de la estructura de discos y particiones. Permite definir volúmenes lógicos (LV), que constituyen una lógica que puede agregar varias particiones físicas que pueden incluso encontrarse en diferentes discos. Esta separación permite, entre otras cosas, cambiar dinámica-mente el tamaño de un LV.

- Conceptos principales:
    - Physical volume (PV), una partición de tipo LVM.
    - Volume group (VG), un conjunto de PV.
    - Logical volume (LV), una parte de un VG, que será formateado y montado para su uso.
- Comandos para la gestión de volúmenes:
    - Físicos:
        - pvcreate <partitions> : Da el formato LVM a las particiones indicadas.
        - pvs : Imprime los volúmenes físicos del sistema.

- pvdisplay <partition> : Muestra información de la partición física especificada, o de todas las particiones físicas si no se ha especificado ninguna partición en concreto.

- pvscan : Devuelve todos los volúmenes físicos existentes.

- Grupos:

  - vgcreate <name> <partitions> : Crea un conjunto de particiones en el que se incluyen las particiones que se pasan como argumento. Da el formato LVM a las particiones que estén sin formatear.

  - vgs : Imprime los grupos de volúmenes del sistema.

  - vgdisplay <groupName> : Muestra la información asociada al grupo de volúmenes especificado. Si no se especifica ninguno, se muestra la información de todos los grupos de volúmenes del sistema.

  - vgscan : Devuelve todos los grupos de volúmenes existentes.

  - vgextend <volumeGroupName> <volumeName> : Añade el volumen en el grupo de volúmenes.

  - vgreduce <volumeGroupName> <volumeName> : Comando que elimina el volumen especificado del grupo de volúmenes especificado.

- Lógicos:

  - lvcreate <volumeGroup> : Comando que permite crear particiones lógicas dentro de un grupo de volúmenes.

    - Opciones:

      - -n <volumeName> : Permite establecer el nombre del volumen.

      - -L <sizeOfVolume> : Permite establecer el tamaño del volumen.

      - -l +<int>%<VG / FREE> : Permite expandir el volumen lógico.

  - lvs : Imprime los volúmenes lógicos existentes en el sistema.

  - lvdisplay <logicalVolume> : Muestra la información asociada al volumen lógico especificado. Si no se especifica ninguno, se muestra la información de todos los volúmenes lógicos del sistema.

        - lvextend <logicalVolume> : Comando que permite ampliar el tamaño del volumen lógico especificado.
            - -l +<int>%<VG / FREE> : Permite expandir el volumen lógico.
        - lvreduce <logicalVolume> : Comando que permite reducir el tamaño del volumen lógico especificado.

Sistemas de Ficheros Encriptados:

- Por motivos de seguridad (especialmente para dispositivos extraíbles o para almacenar datos importantes) se puede encriptar el sistema de ficheros. En linux se usa LUKS (Linux Unified Key Setup) mediante la utilidad cryptsetup.
- Uso crypsetup:
    - cryptsetup luksFormat <partition> : Formatea la partición como una partición de tipo encriptada.
    - cryptsetup luksDump <partition> : Devuelve información de la partición. Algoritmo de encriptación, identificador del volumen, etc.
    - cryptsetup luksOpen <partition> "<deviceName>" : Habilita que pueda montarse el sistema de ficheros encriptado introduciendo su clave. Este comando recibe como argumentos el dispositivo encriptado y un nombre que se asignará al dispositivo que usaremos para montar el sistema de ficheros. Una vez disponible el dispositivo estará en /dev/mapper.
    - cryptsetup luksClose <deviceName> : Deshabilita el montaje de la partición encriptada.

Sistemas de Ficheros Encriptados:

- En el fichero “/etc/fstab” se definen los sistemas de ficheros que se montan en el arranque.
    - Campos:
        - Identificador único unívoco del dispositivo.
        - Punto de montaje.
        - Tipo de sistema de ficheros.
        - Opciones de montaje:

        - auto : Permite montar con la opción -a, la cual monta todos los sistemas de ficheros citados en /etc/fstab.

        - noatime : No actualiza el tiempo de acceso a nodos índice en cada acceso.

        - noexec : No permite la ejecución de los binarios del sistema de ficheros.

        - nosuid : No reconoce los bits suid y sgid.

        - ro : El sistema de ficheros se monta en modo de solo lectura.

        - rw : El sistema de ficheros se monta en modo de lectura y escritura.

        - defaults : El sistema se monta con las opciones predeterminadas.

    - dump : Campo que utiliza el programa dump para decidir cuando hacer una copia de seguridad. 0 Indica que se debe hacer una copia de seguridad del sistema de ficheros, 1 indica que si se ha de realizar.

    - pass : Este campo lo utiliza el programa fsck para decidir el orden en el que los sistemas de ficheros han de ser comprobados. 0 Indica que el sistema de ficheros no ha de ser comprobado, 1 se ha de asignar al sistema de ficheros raíz / (root), los demás sistemas de ficheros han de tener asignados 2.

- mount <deviceName> <direcctoryName> : Por defecto devuelve que sistemas de ficheros están montados. También permite montar un sistema de ficheros si se le indica el dispositivo en el que se encuentra y una carpeta que actúe como punto de montaje del sistema de ficheros.

    - Opciones:

        - -t <fileSystemType> : Permite especificar el tipo de sistema de ficheros que se está montando.

        - -o <mountOptions> : Permite especificar las opciones para el montaje del sistema de ficheros.

TEMA 6: MONITORIZACIÓN DEL SISTEMA

- NOTAS:
  - Si un proceso está en primer plano tiene el control de la terminal y recibe su entrada a través de esta, también recibe las señales generadas por teclado.
  - CTRL + C → Mata el proceso (Señal de interrupción por teclado).
  - CTRL + Z → Manda una señal de parada al proceso.
  - Si un proceso necesita coger los datos de su entrada estándar pero este no tiene el control de la terminal, la shell detiene el proceso.
  - Broken Pipe Signal → Esta señal se muestra cuando se intenta redireccionar un flujo de datos a otro proceso que ya no existe.
  - Si un proceso pierde a su padre INIT lo adopta para que no quede zombi en las tablas de ejecución de procesos del kernel. También podría ser que el proceso estuviera programado para que al morir sus hijos mueran con el.
  - Core Dumped → Es la imagen en memoria de un proceso, contiene su estado de ejecución.

Control de trabajos en la shell:

- jobs : Muestra una lista con todos los procesos que se están ejecutando en segundo o en primer plano. Si la lista está vacía, no hay procesos ejecutándose. “+” identifica al último proceso en ejecutarse, “-” identifica al proceso anterior a este.
  - Opciones:
    - -l : Lista el identificador de los procesos.
- fg [%]<int> : Ejecuta en primer plano el proceso cuyo índice es alguno de los de la lista que ofrece el comando “jobs”. Si se especifica el “%”, el se ejecuta en segundo plano todos los procesos suspendidos o el especificado por un número índice de “jobs”. Si no se especifican parámetros, entonces se muestra un listado con los procesos que están ejecutándose en primer plano.

- bg [%]<int> : Ejecuta en segundo plano el proceso cuyo índice es alguno de los de la lista que ofrece el comando “jobs”. Si se especifica el “%”, el se ejecuta en primer plano todos los procesos que se ejecutan en background o el especificado por un número índice de “jobs”. Si no se especifican parámetros, entonces se muestra un listado con los procesos que están ejecutándose en primer plano.

- nohup <command> : Lanza un proceso que se ejecuta de forma independiente a la sesión de la consola. Esto implica que aunque la consola se cierre, el proceso seguirá ejecutándose. La salida de este programa que de forma normal sería redireccionada a la consola, es redireccionada al fichero “nohup.out”.

- man 7 signal : Muestra una página del manual de GNU/LINUX con todas las señales que pueden emitir o recibir los procesos del sistema.

    - Algunas señales comunes:

Signal	Value	Action	Comment
SIGHUP	1	Term	Cerrar los procesos que cuelgan de la terminal.
SIGINT	2	Term	Interrumpe un proceso por teclado (CTRL + C).
SIGQUIT	3	Core	Termina un proceso por teclado (Core) (CTRL + \).
SIGKILL	9	Term	Hace que un proceso finalice de forma inmediata.
SIGTSTP	18,20,24	Stop	Pasa a suspensión un proceso (CTRL + Z).
SIGCONT	19,18,25	Cont	El proceso debe continuar si está en suspensión.

- Kill <[-]signal/[-]signalValue> <PID’s/-PGID’s> : Envía una señal para finalizar uno o más procesos. En lugar de especificarse los PID de los procesos, también es posible especificar los job mediante jobs %n. Si usamos el “-” entonces la señal se va a usar con el identificador de grupo para matar un conjunto de procesos. Por defecto cada proceso constituye su propio grupo.

    - Opciones:

        - -l : Lista todas las señales.

- pgrep <textPattern> : Lista los PID uno o más procesos cuyo nombre coincida con el patrón de texto especificado.

    - Opciones:

        - -l : Muestra el PID y el nombre de un proceso.

- pkill <[-]signal / [-]signalValue> <textPattern> : Envía una señal a todos los procesos cuyo nombre coincida con el patrón de texto especificado.

- top : Proporciona información sobre los procesos del sistema y el consumo que hacen de la memoria.
    - Comandos interactivos:
        - h : Muestra el menú de ayuda.
        - u : Pregunta el usuario por el que filtrar.
        - k : Pide el PID de un proceso y una señal que se le enviará.
        - q : Salir del programa.
- lsof : Permite ver los descriptores que tiene abierto un proceso.
    - Opciones:
        - -ni : Muestra los ficheros de los sockets.
        - -p <pid> : Muestra los ficheros abiertos por el proceso con el pid dado.
        - -u <userName> : Muestra los ficheros abiertos por el usuario.
        - <File> : Procesos que tienen abierto para escritura el fichero.
        - +D <directory> : Visualizar los archivos abiertos del directorio.

Monitorización de la memoria y entrada/salida:

- vmstat : Imprime información sobre el uso de la memoria.
  - Información:
    - Proc:
      - r : Procesos en espera de ser ejecutados.
      - b : Procesos en suspensión.
    - Memory (KB’s):
      - swpd : Memoria virtual utilizada.
      - fre : Memoria inactiva.
      - buff : Memoria utilizada como buffers.
      - Cache : Memoria caché.
      - Inactive : Memoria inactiva.
      - Active : Memoria activa.
    - Swap (KB’s):
      - si : Memoria intercambiada desde el disco.
      - so : Memoria intercambiada hacia el disco.
    - IO:
      - bi : Bloques recibidos de dispositivos de bloques por segundo.
      - bo : Bloques enviados a dispositivos de bloque por segundo.
    - System:
      - in : Interrupciones por segundo.
      - cs : Cambios de contexto por segundo.
    - CPU:
      - us : % de tiempo de CPU consumido por procesos del usuario.
      - sy : % de tiempo de CPU consumido por procesos del sistema.
      - id : % de tiempo de CPU en inactividad.
      - wa : % de tiempo de CPU en espera de E/S.

- iostat : Muestra estadísticas del rendimiento del subsistema de entrada salida.
    - avg-cpu:
        - %user: % de tiempo de CPU consumido por procesos del usuario.
        - %nice: % de utilización de la CPU cuando se ejecuta con prioridad.
        - %system: % de tiempo de CPU consumido por procesos del sistema. %iowait: % de tiempo de CPU en espera de E/S.
        - %steal: % de tiempo en espera involuntaria de la CPU.
        - %idle: % de tiempo que la CPU estuvo inactiva y sin peticiones E/S.
    - Device:
        - tps: Información transferida por segundo.
        - kB_read/s: Kilobytes leídos por segundo.
        - kB_wrtn/s: Kilobytes escritos por segundo.
        - kB_read: Total de kilobytes leídos.
        - kB_wrtn: Total de kilobytes escritos.

Automatización de procesos con cron y at:

Es el sistema de automatización el que permite ejecutar procesos a una hora y con una determinada periodicidad. Normalmente el demonio responsable de esta tarea es cron, aunque CentOS usa anacron para equipos que se apagan regularmente. La programación de tareas se especifica en /etc/crontab. En cada línea especifica una variable o una tarea mediante 5 parámetros.

NOTAS:

- * indica cualquier valor posible.
- Los campos se separan por espacios.
- Se puede especificar más de un valor separando por comas sin espacios entre medias de los valores.
- Se puede especificar un rango de valores con “-”.
- */<int> múltiplos del número especificado.

SINTAXIS:

- Minuto Hora DíaDelMes Mes DiaDeLaSemana <user> <command>

OTROS FICHEROS:

- crond.d Es el directorio que contiene ficheros al estilo de /etc/crontab para definir la programación de tareas.

- Algunos ficheros de cron.d:

  - 0hourly → Ejecuta las tareas del fichero /etc/cron.hourly cada hora.

  - raid-check → Ejecuta semanalmente una comprobación del disco.

- Ficheros definidos en /etc:

  - /etc/cron.daily: Sus tareas se ejecutarán una vez todos los días.

  - /etc/cron.hourly: Sus tareas se ejecutarán cada hora.

  - /etc/cron.monthly: Sus tareas se ejecutarán cada mes.

  - /etc/cron.weekly: Sus tareas se ejecutarán cada semana.

- COMANDOS:

  - crontab : Permite visualizar, instalar o des-instalar un fichero de crontab.

    - Opciones:

      - -e : Permite editar o crear el fichero de crontab del usuario actual.
      - -l : Muestra el contenido del fichero de crontab para el usuario actual.

  - at [options] [modifiers] <time> [date] [< fileName] : Abre un editor para escribir un conjunto de comandos que serán ejecutados en el tiempo y la hora especificados. Se puede especificar un fichero si se quiere guardar los comandos por algún motivo.

    - Options:
      - -c <int> : Muestra la tarea con el número de job especificado en -l.
      - -l : Lista las tareas programadas para el usuario actual.
      - -d <int> : Elimina la tarea con el número de job especificado en -l.

    - Time: __:__
    - Date: Mes Día Año | Día de la semana | today / tomorrow.
    - Modifiers:
      - <now/teatime/noon/midnight> <+/-> <int>
      - <minutes/hours/days/weeks/months/years>

Logs del sistema:

Una parte importante del mantenimiento de un sistema es monitorizar las acciones que ocurren en él. Los archivos de log recogen esta información y son gran ayuda cuando es necesario analizar un problema. En general los procesos usan una infraestructura común de logging mediante el interfaz syslog. Estos mensajes son procesados por los servicios de logs del sistema, en CentOS 7 hay dos servicios configurados por defecto: journalctl (systemd) y rsyslogd.

- syslog: Es un estándar utilizado para procesar y capturar los mensajes del istema. Todos los mensajes del sistema son etiquetados con un código de identificación (auth, authpriv, daemon, cron, ftp, lpr, kern, mail, news, syslog, user, uucp y local0 hasta local7), el tipo de programa que generó los mensajes y el nivel de severidad del mensaje (Emergency, Alert, Critical, Error, Warning, Notice, Info y Debug). Este mecanismo registra los mensajes del sistema en un conjunto de ficheros descritos en /etc/rsyslog.conf.

- En /etc/rsyslog.conf se define en que fichero de /var/log se ha de registrar cada mensaje del sistema. Cada línea contiene un mensaje y su código de prioridad.

    - Algunos de los ficheros de /var/log son:

        - dmesg → Contiene los mensajes del kernel.
        - boot.log → Mensajes relacionados con el inicio del sistema.
        - secure → Mensajes relacionados con la seguridad del sistema.
        - messages → Contiene los mensajes relacionados con el sistema de red.

    - Niveles de importancia de los mensajes:

        - LOG_EMERG → El sistema está inservible.
        - LOG_ALERT → Una acción debe ser realizada de inmediato.
        - LOG_CRIT → Condiciones críticas.
        - LOG_ERR → Condiciones de error.
        - LOG_WARNING → Condiciones de aviso.
        - LOG_NOTICE → Condiciones normales pero significativas.
        - LOG_INFO → Mensajes informativos.
        - LOG_DEBUG → Mensajes de depuración.

- rsyslogd: Comando de administración que proporciona funciones de registro local y remotos.

- dmesg: Comando de administración que muestra los mensajes del kernel.

- logrotate : Comando de administración del sistema diseñado para mantener los ficheros de log del sistema. Herramienta pensada para trabajar sobre ellos.

- systemd introduce una nueva filosofía de logging que reemplaza el sistema de log en texto plano por una base de datos en binario.

    - journalctl : Comando principal de acceso al log del sistema que gestiona systemd, permitiendo ver todos los mensajes del sistema, así como de todos los servicios y usuarios.

        - Opciones:

            - -n <int> : Muestra los últimos n.º mensajes.
            - -f : Muestra los mensajes de forma continua.
            - -b : Muestra los mensajes del arranque actual.
            - -x : Muestra mensajes de log más explicativos.
            - -p <7-0> : Muestra los mensajes con la prioridad especificada.
            - -e : Muestra la página con los últimos mensajes, los más recientes.
            - -u <serviceUnit> : Muestra los mensajes relacionados con el servicio.
            - --until=”format string” | --since=“format string”: Muestra los mensajes hasta el momento de tiempo especificado. “5 minutes ago”.

    - El comportamiento de journal se puede configurar en el fichero del sistema /etc/systemd/journald.conf

TEMA 7: ADMINISTRACIÓN DE LA RED Y SERVICIOS BÁSICOS

Conceptos básicos de redes:

- Modelo OSI:
  - Capa 7 (Capa de aplicación): Capa que ofrece servicios a los usuarios.
    - DNS: Protocolo que traduce nombres de dominio a direcciones IP.
    - DHCP: Protocolo de red usado en arquitecturas cliente servidor. El servidor provee a los clientes una lista de direcciones IP dinámicas y las ofrece a los clientes en función de la disponibilidad de estas. Lleva un registro de a quien se le ha asignado una IP, durante cuanto tiempo y a quien se le ha asignado después, etc. Supone un avance para la configuración automática de la red.
    - SSH: Protocolo que permite realizar conexiones seguras.
  - Capa 6 (Capa de presentación): Capa que se ocupa del transporte, compresión y cifrado.
  - Capa 5 (Capa de sesión): Capa responsable de controlar el diálogo y la sincronización.
  - Capa 4 (Capa de transporte): Es la responsable de la entrega de un mensaje desde un proceso a otro.
  - Capa 3 (Capa de red): Es el responsable de la entrega de tramas individuales desde un host origen a host destino.
    - TCP: Protocolo que garantiza que los datos que un cliente transmite a un servidor son fiables. Revisa que los datos no tengan errores y que se reciben en el mismo orden en que fueron transmitidos.
    - IP: Protocolo responsable del direccionamiento y la fragmentación de paquetes de datos.
    - PING: Utilidad para comprobar el estado de la comunicación entre equipos. Utiliza para ello el envío de paquetes de solicitud (ICMP Echo Request) y respuesta (ICMP Echo Reply).

    - Capa 2 (Capa de enlace de datos): Se ocupa del movimiento de las tramas desde un nodo de la red al siguiente.
        - ARP: Protocolo que obtiene la dirección física MAC de un dispositivo a partir de su dirección IP.
    - Capa 1 (Capa física): Incorpora lo necesario para la transmisión de datos sobre un medio físico. Trata con las especificaciones eléctricas y mecánicas de la interfaz harware y del medio de transmisión.

- Dirección IP: Número binario que diferencia a una máquina de las del resto de una red. El formato más común es IPv4 que emplea direcciones de 32 bits.

- Máscara de red: Cadena de bits que indica que parte de la dirección IP es es número de red (y subred) y que parte es la que corresponde al host.

- Tipos de redes:
    - Clase A: 8 bits de red y 24 bits de host.
    - Clase B: 16 bits de red y 16 bits de host.
    - Clase C: 24 bits de red y 24 bits de host.

- MAC-ADDRESS: Dirección física. Es un identificador unívoco que poseen todos los dispositivos conectados a una red.

- Socket: Descriptor de fichero que representa una conexión de red mediante la una IP y un puerto local.

Comandos para configurar manualmente el entorno de red:

- ip : Comando que permite manipular los dispositivos de red y de enrutamiento.
  - Opciones:
    - -s : Muestra estadísticas sobre la transferencia o el recibo de bytes de las distintas interfaces de red.
- ip l/link [show interfaceName]: Permite ver los interfaces de red del sistema y el estado en el que se encuentran. El estado puede ser UP o DOWN dependiendo si la interfaz de red está activa o no. Si no se especifica que interfaz de red que se ha de mostrar, entonces se mostrarán todas.
  - Nomenclatura de interfaz: <interface_type>p<pci_number>s<slot_number>
    - Tipos de interfaz:
      - en : EtherNet. Interfaz de red cableada.
      - wl : WirelessLan. Interfaz de red inalámbrica.
      - lo : LoopBack. Interfaz usada para probar servicios web en local.
    - PCI: Es un modelo de bus estandarizado para conectar dispositivos directamente a la placa base.
    - SLOT: Ranura en la que un dispositivo es conectado.

- ip link set <interfaceName> … : Permite realizar ajustes sobre dispositivos de red.
    - Usos:
        - up/down : Activa o desactiva el interfaz de red especificado.
        - name “newInterfaceName” : Cambia el nombre de la interfaz de red por el especificado.
        - mtu <int> : Establece el MTU, que es la máxima cantidad de bytes que pueden transferirse empleando un determinado protocolo de comunicaciones. Para Ethernet el máximo es 1.500 bytes
- ip a/addr/address … :
    - show networkInterface : Muestra las direcciones MAC (link), IPv4 (intet) y IPv6 (inet6) de la interfaz de red especificada. Si no se especifica ninguna, se mostrarán las de todas.
    - add <IPv4> dev <interfaceName> : Añade un nuevo protocolo de direccionamiento al dispositivo especificado. Las máscaras de red se especifican de la forma ___.___.___.___/<int> donde el entero especificado es la máscara que se aplica a la IP.
- ip r/rou/route : Muestra la tabla de enrutamiento, que es un fichero que contiene las rutas a los diferentes dispositivos de una red.

- ip n/nei/neigh/neighbour … : Gestor de tablas ARP. Este protocolo se ocupa de realizar la resolución de direcciones para obtener la dirección física (MAC) a partir de la dirección IPv4, ya que para que pueda establecerse una comunicación entre dos máquinas es necesario disponer de sus direcciones físicas.

    - show [IPv4] : Muestra el contenido de las tablas ARP, estas contienen las direcciones IPv4 y las direcciones físicas (MAC) de los host con los que se ha mantenido una conexión. Si no se especifica una dirección IPv4, se muestran todas las direcciones IPv4 de los host así como sus respectivas direcciones físicas.

    - add/del <IPv4> lladdr <MAC> dev <networkInterface> nud <state> : Añade o elimina una entrada de la tabla de vecinos.

        - lladdr : Define una dirección de capa de enlace para una entrada de la tabla de vecinos.

        - dev : Dispositivo de red sobre el que se aplica el comando.

        - nud : Permite especificar el estado de detección de los vecinos.

        - state :

            - noarp : Marca la entrada como válida y como no marcada. Puede ser eliminada cuando expire.

            - permanent : Como noarp, pero una entrada permanente solo la puede eliminar un administrador.

            - reachable : Marca la entrada como valida hasta que expire su límite temporal de alcance.

            - stale : Marca una entrada nueva o cambiada como válida, pero sospechosa. El kernel verificará estas entradas en la primera transmisión.

    - flush <all/IPv4> : Borra la entrada especificada de la tabla de vecinos mediante una dirección IPv4, también puede especificarse que se borren todas las entradas de la tabla de vecinos si se especifica la opción “all”.

- ping <IPv4> : Este comando permite averiguar si podemos alcanzar un host remoto. Si un ping es contestado, sabemos que la capa de red está funcionando.
    - Opciones:
        - -t <int> : Establece el tiempo de vigencia de la ip al número de segundos especificados.
        - -c <int> : El comando se detiene después de enviar y recibir el número de paquetes especificado.
        - -s <bytes> : Tamaño del paquete (número de bytes de datos a enviar). Por defecto es 56, que se transforman en 64 al combinarse con los otros 8 de la cabecera ICMP.
- tcpdump [protocol] [src/dst direction] [port <int/int and int>] : Comando que captura paquetes del tráfico de red. El comando no termina hasta que no hay una interrupción por teclado (Ctrl + C). Una vez interrumpido genera un informe sobre el tráfico de red capturado.
    - Opciones:
        - -A : Imprime los paquetes como texto ascii.
        - -D : Imprime una lista con las interfaces disponibles y luego finaliza.
        - -i <netwrokInterface> : Escucha en la interfaz de red especificada. Su valor por defecto es “any”, es decir, se pone capturar el tráfico de todas las interfaces de red.
        - -n : Muestra en los resultados las direcciones IP en lugar de los nombres de los host.
    - Protocol : Filtra por paquetes de un protocolo de comunicaciones (ip, ip6, tcp …).
    - src/dst direction : Indica que queremos capturar los paquetes cuyo orrigen/destino sean los de la dirección especificada.
- host <hostName/hostIP> : Imprime información sobre el host especificado.

Archivos de configuración de red:

- La configuración global de la red se puede configurar en: /etc/sysconfig/network

- El servicio, network configura los interfaces de red definidos cuando arranca el sistema operativo. Con systemctl podemos ver su estado (state), pararlo (stop) o hacer que vuelvan a cargarse las configuraciones de los dispositivos de red (restart).

- La configuración por defecto de cada interfaz de red se guarda en un archivo separado en la ruta: /etc/sysconfig/network-scripts/ifcfg-<dev>

- ifup <networkInterface> : Levanta la interfaz de red especificada aplicando la configuración de /etc/sysconfig/network-scripts/ifcfg-<dev>

- ifdown <networkInterface> : Desactiva la interfaz de red especificada.

- Configurar los interfaces de red: /etc/sysconfig/network-scripts/ifcfg-<dev>

    - Configuración dinámica (DHCP):

      DEVICE=enp0s3
      BOOTPROTO=dhcp
      ONBOOT=yes

    - Configuración estática (IPv4 fija):

      DEVICE=enp0s3
      BOOTPROTO=none
      ONBOOT=yes
      NETWORK=192.168.0.0
      NETMASK=255.255.255.0
      IPADDR=192.168.0.1

- Significado de los campos:
  - DEVICE : Dispositivo de red.
  - BOOTPROTO : Establece el protocolo con el que ha de trabajar la interfaz de red. Protocolos posibles: none, dhcp, bootp …
  - ONBOOT : “yes” indica que el dispositivo de red debe inicializarse durante el arranque del sistema operativo, “no” sería lo contrario.
  - NETWORK : Dirección de la red.
  - NETMASK : Máscara de red.
  - IPADDR : Dirección IPv4.
- Otros campos:
  - BROADCAST : Dirección de difusión.
  - GATEWAY : Dirección del dispositivo que hace de router (puerta de enlace).
  - HWADDR o MACADDR : Dirección física del dispositivo.

Resolución de nombres:

- La resolución de nombres se configura en /etc/resolv.conf. Este archivo contiene los servidores DNS (nameserver) y el dominio por defecto (search).
  - search: Permite indicar un nombre de dominio por fefecto.
  - nameserver: Dirección IP del servidor cuyo nombre queremos usar. Es posible usar más de un nombre para un mismo servidor, lo normal es usar dos, un nombre primario y otro secundario.
- /etc/hosts : Archivo que contiene los nombres de las máquinas y sus respectivas direcciones IPv4.
- /etc/nsswitch.conf : Es el fichero que determina si se usa DNS o /etc/hosts
  - hosts: files dns → Indica que un host se busque primero en /etc/hosts y si no se encuentra, que se busque por DNS.

Configuración dinámica de los host:

- El protocolo DHCP permite configurar la red de un host, sus direcciones IP, servidores DNS, etc.

- El servicio dnsmasq puede implementar un servidor DHCP, un proxy DNS, etc.

    - Este servicio se configura en /etc/dnsmasq.conf

        - dnsmasq permite establecer el rango de direcciones IP dinámicas que puede prestar para que los host realizen sus conexiones, así como el tiempo que un determinado host puede utilizar la IP que el servidor DHCP le ha prestado.

            - dhcp-range=IP_LOW,IP_TOP,NETWORK_MASK,IP_DURATION

- dhclient <networkInterface> : Comando para configurar los enlaces de red con el protocolo DHCP.

    - Opciones:

        - -v : Habilita que los mensajes de log del sistema sean más detallados.

        - -x: Detiene el cliente DHCP.

Monitorización de la red:

- ss [state <conexionState>] : Es una utilidad para trabajar con sockets. Permite extraer información de las conexiones de red y de los puertos abiertos.

    - Opciones:

        - -a : Muestra información de todos los socket.

        - -t : Muestra todas las conexiones TCP.

        - -u : Muestra todas las conexiones UDP.

        - -p : Muestra los procesos que están haciendo uso de un socket.

        - -n : Muestra el número de puerto en lugar del protocolo que lo usa.

- lsof : Herramienta que permite ver que archivos están abiertos por procesos.
    - Opciones:
        - -i : Muestra los sockets abiertos.
- En el fichero /etc/services se definen los puertos más conocidos y que protocolos los utilizan.

Acceso remoto seguro:

- ssh <remoteUser>@<remoteHost> : Proporciona una conexión segura a un host remoto, permitiendo ejecutar comandos en dicho host.
    - Opciones:
        - -L <localPort:remoteHost:remotePort> : Permite establecer una conexión ssh desde un puerto local a un puerto de un host remoto.
- scp <file> <remoteUser>@<remoteHost>:<file> : Copia con seguridad ficheros entre hosts de una red mediante el uso del protocolo ssh. El primer parámetro es el fichero del sistema origen, este viene seguido por el usuario remoto y el host remoto al que enviar el archivo, por último se especifica la ruta y el nombre donde se copiará el archivo en el sistema remoto.
- ssh-keygen : Generador de claves de autentificación. Genera los archivos de clave pública (candado) y privada (llave). El archivo de clave pública es el mecanismo de seguridad que evitará que se cometa una suplantación de nuestro usuario en el servidor remoto. Este se le ha de pasar al servidor remoto ya que cuando alguien intente conectase como nuestro usuario, el servidor remoto cogerá nuestro mecanismo de clave pública pasado anteriormente y sólo se desbloqueará si desde nuestro lado le ofrecemos el archivo con nuestra clave privada. La clave pública se añade al fichero authorised del host remoto.
- ssh-copy-id <remoteUser>@<ipHost / hostName> : Mecanismo para copiar de forma segura nuestra clave pública en un host remoto de la red.
    - Opciones:
        - -i <privateKeyFile> : Para especificar la ruta al fichero de clave privada.
- El servidor ssh puede configurarse desde el fichero /etc/ssh/sshd_config
    - Para deshabilitar el login como root: PermitRootLogin no

Otros comandos:

- lspci : Lista todos los dispositivos periféricos que han sido reconocidos por el kernel del sistema.