

Semana 11:

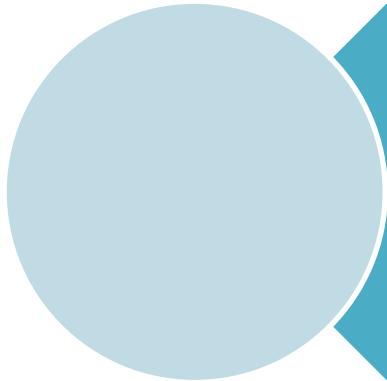
Administración de Usuarios y Grupos

Sistemas Operativos

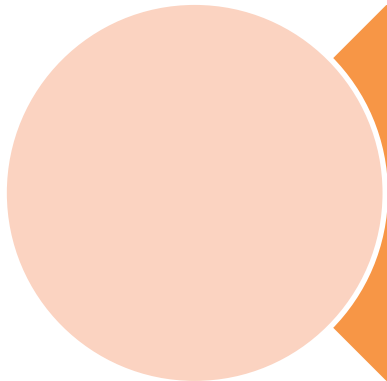
Introducción

- El usuario es un elemento fundamental en el trabajo con un sistema operativo.
- No solo define las credenciales de autenticación que permitirán al usuario ingresar al sistema, sino que asocian los permisos que determinarán las acciones que el usuario podrá realizar.
- En esta unidad trataremos acerca de la administración de usuarios, revisando los diferentes comandos que se tiene para realizar estas tareas.
- Así mismo revisaremos el tema de los permisos, donde se explicará cómo se realiza la asignación de permisos a los usuarios y la implicancia de los mismos.

Capacidades de la Sesión



Gestiona cuentas de usuarios y grupos



Administra cuentas de usuarios y grupos.

Cuenta de Usuario

- Una cuenta de usuario, representa a una persona o grupo de personas.
- A esta cuenta, se le asigna un conjunto de permisos sobre un sistema en particular.
- Una cuenta de usuario consta de:

- Nombre de usuario (login name)
- Nombre real
- Contraseña
- Permisos



Login	: jdiaz
Nombre	: Juan Diaz
Contraseña	: *****
Permisos	:

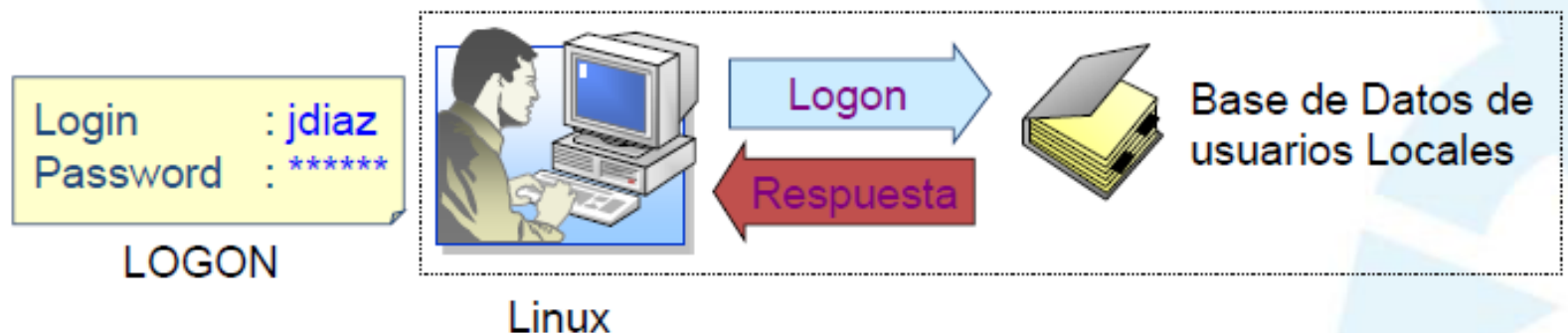
Uso de la Cuenta de Usuario

- La cuenta de usuario es utilizada para permitir el acceso a los recursos de un equipo Linux.



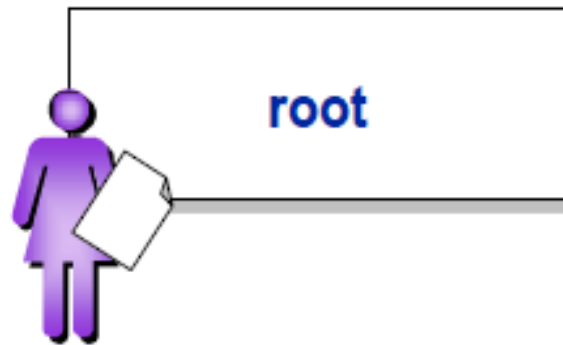
Tipos de Validación

- La comprobación de la validez de una cuenta de usuario puede ser realizada en el mismo servidor(Host):
 - El usuario ingresa su nombre y su contraseña en el servidor.
 - En el servidor se verifica si los datos coinciden con los almacenados en su base de datos.
 - Si los datos son incorrectos, se envía un mensaje de error al usuario. Si los datos son correctos, se inicia una sesión para el usuario, activando los permisos asignados a dicho usuario.



Cuentas de Usuario por Defecto

- Al configurarse Linux, se crean automáticamente algunas cuentas de usuario, como las siguientes:
 - root
 - bin
 - daemon
 - adm, etc.



Planificación de Nombres para las Cuentas de Usuarios

- El administrador debe definir los parámetros necesarios para la creación, mantenimiento y eliminación de cuentas de usuarios.
- Definirá el formato de nombre que las cuentas de usuarios utilizarán.
- Por ejemplo:
 - Formato: **abbb....bxx**
 - a: Es la primera letra del nombre
 - bb...b: Es el apellido completo del usuario
 - xx: Es el número a utilizar en caso de duplicidad
 - Aplicación:
 - El nombre de usuario para **Juan Díaz** será **JDIAZ**.

Identificadores Únicos de Cuentas de Usuarios

- Los nombres de usuario son típicamente en minúsculas y con un máximo de 8 caracteres.
- Cada cuenta de usuario tiene un único identificador (UID: User ID).
- Los números de UID mayores o igual a 500 son asignados a los usuarios comunes. Los números menores a 500 son reservados para cuentas del sistema:
 - UID 0 root
 - UID 1 bin
 - UID 2 daemon
 - UID 3 adm



Cuentas de Usuario Predeterminadas

- Root UID=0
 - Súper usuario, utilizado por el administrador del sistema.
 - No tiene restricciones.
- Bin UID=1
 - El propietario de muchos de los programas ejecutables.
- Daemon UID=2
 - El propietario de muchos de los demonios del sistema.

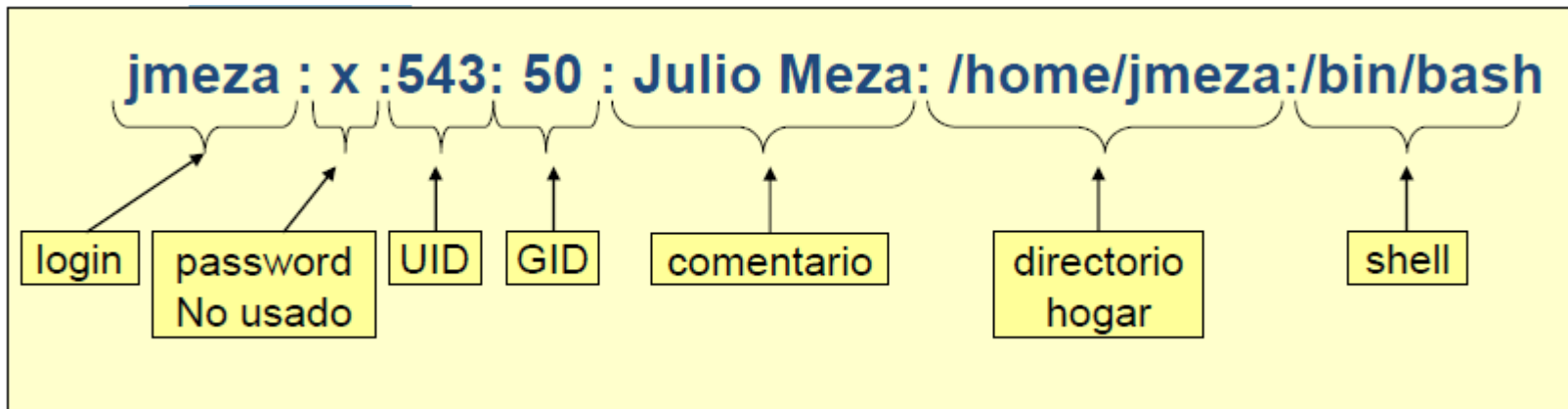
Información Contendida en las Cuentas de Usuarios

- Una cuenta consiste en toda la información que requiere un usuario para poder pertenecer al sistema Linux:
 - *Nombre de Cuenta (Login name)*
 - *Contraseña (password)*
 - *Identificación del usuario (UID)*
 - *Identificación del grupo (GID)*
 - *Directorio Hogar (Home directory)*
 - *Correo electrónico (Mail)*
 - *Archivos de Inicio*



Archivo de Cuentas `/etc/passwd`

- La información de las cuentas se encuentra en el archivo `/etc/passwd`. Sus características son:
 - Es un archivo de texto
 - Permiso de lectura para todos los usuarios.
 - Solo el súper usuario (root) puede modificarlo.
 - Cada línea contiene la información de un usuario:



Archivo de Cuentas /etc/passwd

- Algunos registros de /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
```

Archivo de Contraseña `/etc/shadow`

- Las contraseñas de los usuarios se encuentran cifradas en el archivo `/etc/shadow`. Sus características son:
 - Es un archivo de texto
 - Solo el súper usuario (root) puede modificarlo.
 - Cada línea contiene la información de un usuario:

jmeza:\$1\$PK4M\$9feuvlruyQU7:last:min:max:warm:inact:expire:nouse

login

password

envejecimiento

Archivo de Contraseña /etc/shadow

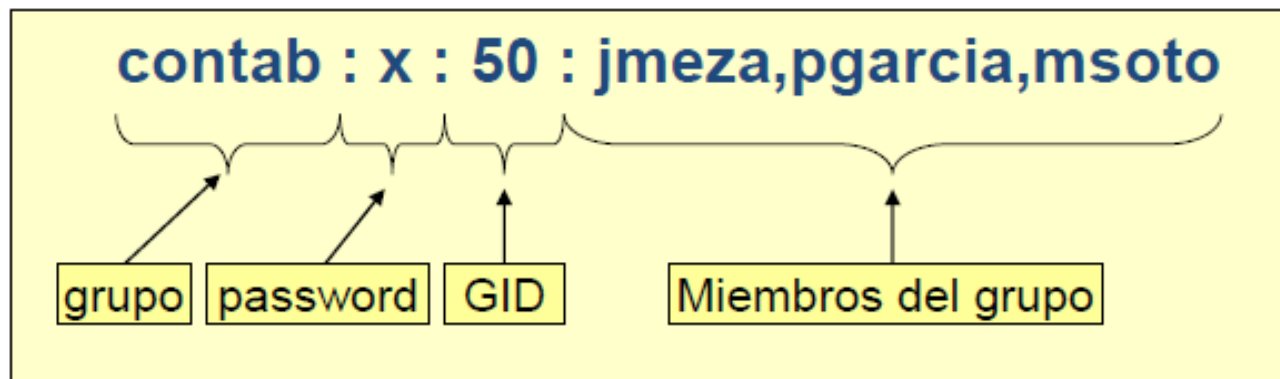
```
root:$1$0NcBT0Zn$RVpGvRTN.HTyuAWPkRFSX1:13256:0:99999:7:::  
bin:*:13256:0:99999:7:::  
daemon:*:13256:0:99999:7:::  
adm:*:13256:0:99999:7:::  
lp:*:13256:0:99999:7:::  
sync:*:13256:0:99999:7:::  
shutdown:*:13256:0:99999:7:::  
halt:*:13256:0:99999:7:::  
mail:*:13256:0:99999:7:::  
news:*:13256:0:99999:7:::  
uucp:*:13256:0:99999:7:::  
operator:*:13256:0:99999:7:::  
games:*:13256:0:99999:7:::  
gopher:*:13256:0:99999:7:::  
ftp:*:13256:0:99999:7:::  
nobody:*.13256.0.99999.7...
```

Valores de Envejecimiento en el Archivo /etc/shadow

- **last:** Cuántos días desde 01/01/1970 han pasado desde el último cambio de contraseña.
- **min:** Tiempo de vida (días) mínimo de la contraseña.
- **max:** Tiempo de vida (días) máximo de la contraseña.
- **warn:** Cuántos días antes de la expiración de la contraseña, se notificará al usuario.
- **inactive:** Días después de la expiración de la contraseña en que la cuenta será deshabilitada.
- **expire:** Días desde el 01/01/1970 cuando la cuenta expira.
- **reserved:** Campo reservado.

Grupos

- Cada usuario puede pertenecer a uno o a varios grupos.
- La relación de grupos válidos se encuentran guardados en el archivo **/etc/group**
- Este archivo contiene una entrada para cada grupo disponible.



Grupos

- Algunos registros de /etc/group

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
```

Identificadores de Grupos

- Los identificadores de grupo (GID) **menores** de 500 son reservados para los **grupos del sistema**:
 - GID 0rootGID 2daemon
 - GID 1binGID 3sys
- Los identificadores de grupo (GID) **mayores** o igual a 500 se usan para los **grupos creados por usuario**.

Administración de Usuarios y Grupos

Creación de Usuarios

- Los pasos necesarios para crear una cuenta de usuario son:
 - Editar el archivo `/etc/passwd` y agregar la línea correspondiente al usuario a crear.
 - Editar el archivo `/etc/group` y agregar al grupo correspondiente.
 - Crear un directorio hogar para el usuario: `"/home/user"`
 - Copiar los archivos de inicialización (startup) en el directorio hogar creado.
 - Asignar los permisos necesarios sobre los directorios y archivos.
 - Asignar un password inicial para el usuario.



Comando useradd

- El comando **useradd** o **adduser** nos permite crear usuarios así como cambiar algunos de los valores por defecto.
- Para mostrar los valores por defecto use la opción “-D”.
 - Estos valores se encuentran en el archivo: “/etc/default/useradd”.

```
# useradd -D  
GROUP=100  
HOME=/home  
INACTIVE=-1  
EXPIRE=  
SHELL=/bin/bash  
SKEL=/etc/skel
```

Crear Usuarios con Valores por Defecto

- El comando `useradd` le permite crear usuarios rápidamente, sin necesidad de especificar mayores opciones, para lo cual tomará los valores por defecto.
- Ejemplo:

```
# useradd -c "Mario Rojas" mrojas
```

Crear Usuarios con Valores por Defecto

- Este comando realiza las siguientes tareas:

- Añade una entrada en el archivo **/etc/passwd**

```
mrojas:x:536:536:Mario Rojas:/home/mrojas:/bin/bash
```

- Añade una entrada en el archivo **/etc/shadow**

```
mrojas:!!:12297:0:99999:7:::
```

- El directorio **/home/mrojas** será creado y el contenido del directorio **/etc/skel** será copiado ahí.
- Debido a que no se especificó UID, se usará el siguiente UID disponible.
- La cuenta será creada pero el usuario no podrá acceder hasta que se le asigne una contraseña.



Crear Usuarios con Valores Personalizados

- El comando `useradd` contiene una serie de opciones para poder modificar los valores por defecto al momento de crear un usuario.

```
useradd [-u uid [-o]] [-g group] [-G group,...]  
        [-d home] [-s shell] [-c comment] [-m [-k template]]  
        [-f inactive] [-e expire ] [-p passwd] [-n] [-r] name  
useradd -D [-g group] [-b base] [-s shell]  
        [-f inactive] [-e expire ]
```

- Ejemplo:
 - `useradd -u 601 -g 100 -d /home/contab/jaguar -c "JoseAguilar" jaguar`

Modificar Cuentas de Usuario

- Una vez que el usuario ha sido creado usted puede realizar cambios manualmente o usando alguna de las herramientas disponibles.
- Linux provee del comando **usermod** para modificar la información referente a una cuenta de usuario.
 - Este comando tiene similares opciones que el comando **useradd**.
 - Por ejemplo para cambiar el shell del usuario:
usermod -s /bin/tcsh *usuario*
 - Si desea cambiar la fecha de expiración de la cuenta:
usermod -e 09/15/2000 *usuario*

Eliminar Cuentas de Usuario

- La mayoría de sistemas proveen scripts para eliminar usuarios, tales como **userdel**. **userdel *usuario***
- Para eliminar también el directorio hogar, use la opción -r. **userdel -r jaguilar**
- También se puede eliminar un usuario manualmente:
 - Borre la entrada de **/etc/passwd**
 - Borre la entrada de **/etc/shadow**
 - Remueva el login name de los grupos respectivos en **/etc/group**
 - Elimine el directorio hogar



Administrar Grupos

- Para crear un grupo:
`groupadd grupo`
- Para modificar un grupo:
`groupmod [-g GID [-o]] [-n name] grupo`
- Para eliminar un grupo:
`groupdel grupo`
- Para añadir un usuario a un grupo:
`usermod -G grupo usuario`

Asignación de Permisos para Directorios y Archivos

Permisos de Archivo

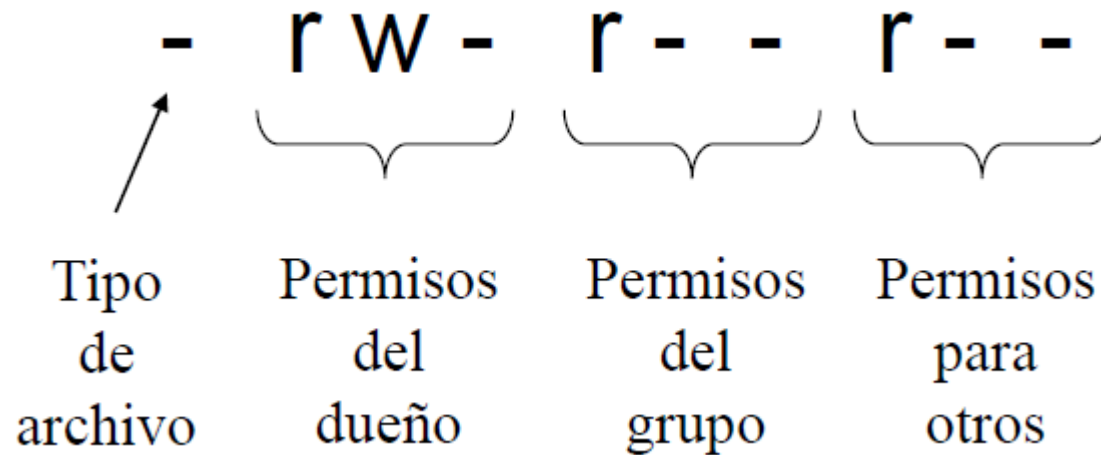
- Los permisos determinan quién puede tener acceso a los archivos y directorios.
- El conjunto de permisos es llamado “modo del archivo”.
- Para visualizar los permisos del archivo utilice el comando **ls-l**
 - El primer carácter de cada línea identifica el tipo de archivo.
 - Los siguientes nueve caracteres de cada línea indican el conjunto de permisos actuales del archivo.

```
ls -l carta
```

```
-rw-r--r--  1 lmendoza  group  1050  Feb 27  carta
```

Categoría de Acceso

- Cada archivo tiene tres categorías de acceso:
 - Dueño o propietario del archivo (dueño).
 - Grupo al que pertenece el usuario (grupo) y,
 - Otros usuarios que tienen acceso al sistema (otros).



Tipos de Permisos

- A cada categoría de acceso le corresponden tres tipos diferentes de permisos:

r	: permiso de lectura
w	: permiso de escritura
x	: permiso de ejecución
-	: permiso denegado

Efectos de los Permisos sobre Archivos y Directorios

Permiso	Archivo	Directorio
r	Abrir el archivo	Ver los archivos en el directorio
W	Modificar el archivo	Crear o eliminar archivos en el directorio
X	Ejecutar un archivo	Buscar y acceder al directorio

Tipos de Asignación de Permisos

- Se puede cambiar de permiso de 2 maneras:
 - Método simbólico
 - Método octal

Cambio de Permiso: Método Simbólico

```
chmod <quién> <acción> <acceso> archivo
```

quién:

- u** - usuario
- g** - grupo
- o** - otros

acción:

- +** (otorga el permiso)
- (elimina el permiso)

acceso:

- r** - lectura
- w** - escritura
- x** - ejecución

Cambio de Permiso: Método Simbólico

```
ls -l texto1
```

```
-rw-r--r-- 1 jmendoza group 2133 Mar 12 texto1
```

```
chmod u+x texto1
```

```
ls -l texto1
```

```
-rwxr--r-- 1 jmendoza group 2133 Mar 12 texto1
```

```
chmod go+w texto1
```

```
ls -l texto1
```

```
-rwxrw-rw- 1 jmendoza group 2133 Mar 12 texto1
```

```
chmod g-w, o+x-r texto1
```

```
ls -l texto1
```

```
-rwxr---wx 1 jmendoza group 2133 Mar 12 texto1
```

Cambio de Permiso: Método Octal

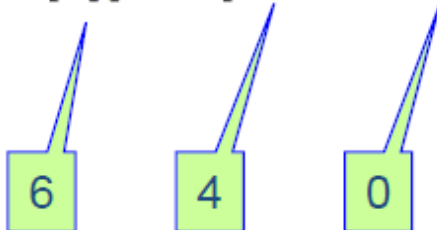
```
chmod <número octal> archivo
```

A cada permiso se le asigna un numero

r = 4 w = 2 x = 1

Ej.:

- rw- r-- --- equivale a 640



Cambio de Permiso: Método Octal

```
ls -l carta
```

```
- rw- r-- r-- 1 jmendoza group 2133 Mar 12 carta
```

6 4 4

```
chmod 751 carta
```

```
ls -l carta
```

```
- rwx r-x --x 1 jmendoza group 2133 Mar 12 carta
```

7 5 1

Efectos del “umask” en Archivos y Directorios

- **umask**, es una comando que define los permisos por defecto para la creación de archivos y directorios.
- El valor es: “022” o “002”.

Archivos :	complemento a	6 6 6	
		0 2 2	

		6 4 4	rw-r--r--
Directorios:	complemento a	7 7 7	
		0 2 2	

		7 5 5	rwXr-Xr-X

Permisos Especiales

- **Stick bit (1xxx):** directorio solo pueden ser renombrados o borrados por su propietario o bien por root. El resto de usuarios que tengan permisos de lectura y escritura, los podrán leer y modificar, pero no borrar.

```
chmod 1775 /test
```

- **SGID(2xxx):** Si se aplica este bit al directorio, cualquier archivo creado en dicho directorio, tendrá asignado el grupo al que pertenece el directorio.

```
chmod 2775 /test
```



Permisos Especiales

- **SUID (4xxx):** es un permiso que se aplica sobre un archivo el cual permitirá que el que lo ejecute va a tener los mismos permisos que el que creó el archivo. Esto es útil en algunas ocasiones, aunque hay que utilizarlo con cuidado, ya que puede acarrear problemas de seguridad

```
chmod 4775 archivo.sh
```

Cambiando de Dueño y Grupo

- El usuario root puede cambiar la propiedad del archivo, es decir darle el archivo a otro usuario, o modificar el grupo al cual pertenece.
- Para ello se utilizan los comandos **chown** y **chgrp** respectivamente.

```
ls -l carta
-rw-r--r-- 1 lmendoza group 1050 Feb 27 carta

chown jsoto carta
chgrp sistemas carta

ls -l carta
-rw-r--r-- 1 jsoto sistemas 1050 Feb 27 carta
```


FIN DE LA UNIDAD

Bibliografía

- Adelstein, Torn (2007). Administración de Sistemas Operativos Linux. Madrid: Anaya Multimedia (005.43L/A23)
- Alegría Loainaz, Iñaki (2005). Linux Administración del Sistema y la Red. Madrid: Pearson Educación (005.43L/A37)
- Negus, Christopher (2013). Linux, Bible. Albany NY: A.De Boeck (005.43L/N36)