Usuarios y Grupos

Usuarios y grupos en Unix

Cuentas de Usuario

Las cuentas de usuario en Unix se dividen en dos partes.
En **nombre de usuario** (Login) y en **contraseña**(password).
Las cuentas son creadas por el administrador de sistema (ROOT). Los usuarios pertenecerán como mínimo a un grupo de usuarios, ay que como mínimo tendrán asignados un grupo primario.

Las cuentas de usuario también ofrecen al usuario una ruta para almacenar sus documentos y su perfil. Esta ruta es **/home/nombre de usuario.** Se le denomina carpeta home del usuario. También se le genera un **shell** que le permite ejecutar aplicaciones.

Con el comando **top** se visualizan todos los procesos en ejecución en el sistema.

Cuando creas un nuevo archivo, el propietario de este es el usuario que lo ha creado y el grupo será el grupo de su mismo nombre.

Una cuenta de usuario permite el acceso a un equipo tanta presencia y tanto por red.
Los sistemas Unix codifican a los usuarios mediante el **uid**, un número que es único de cada usuario. Los usuarios creados parte desde el 1000.
Los menores a 100 son usuarios propios del sistema.

La información de los usuarios se almacena el archivo **/etc/passwd.** El archivo solo puede ser modificado por el usuario root.

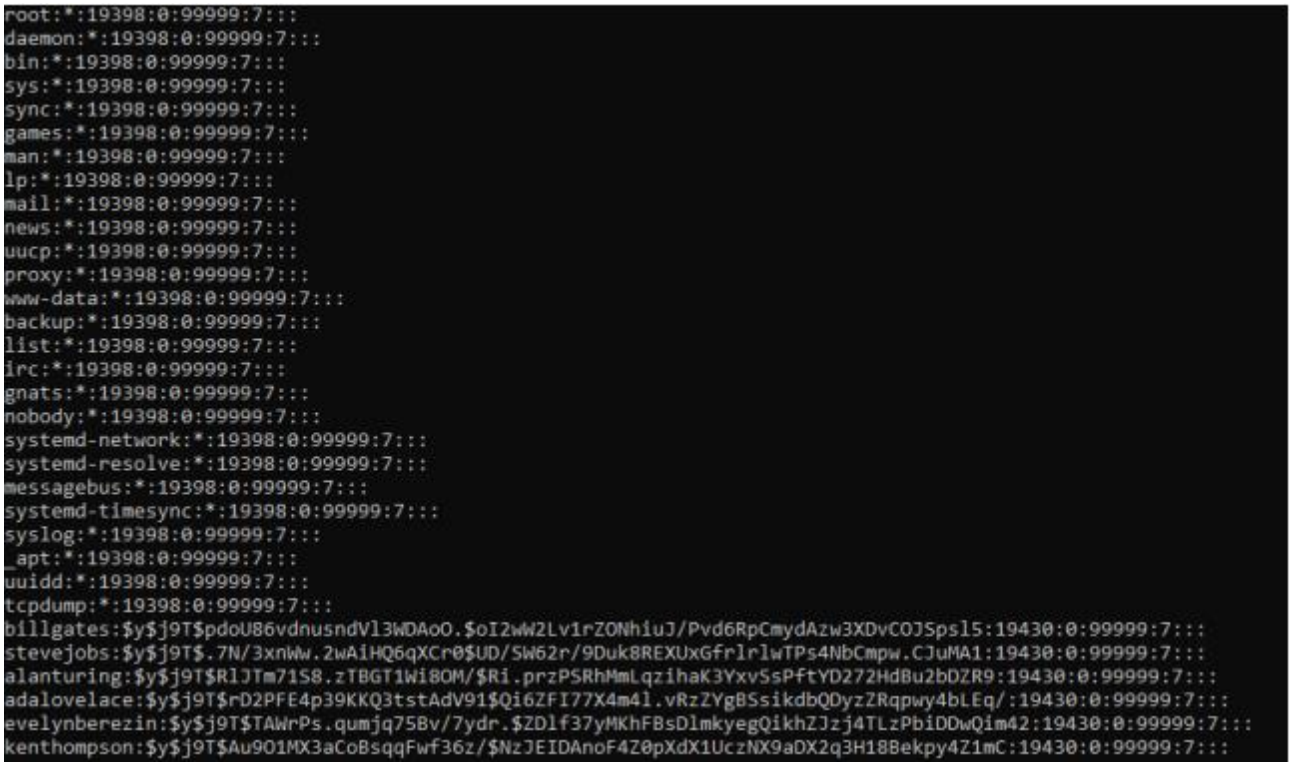
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:106:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:107:113::/nonexistent:/usr/sbin/nologin
billgates:x:1000:1000:,,,:/home/billgates:/bin/bash
stevejobs:x:1001:1001:,,,:/home/stevejobs:/bin/bash
alanturing:x:1002:1002:,,,:/home/alanturing:/bin/bash
adalovelace:x:1003:1003:,,,:/home/adalovelace:/bin/bash
evelynberezin:x:1004:1004:,,,:/home/evelynberezin:/bin/bash
kenthompson:x:1005:1005:,,,:/home/kenthompson:/bin/bash
daniel:x:1006:1006:,,,:/home/daniel:/bin/bash
pablo:x:1007:1011:,,,:/home/pablo:/bin/bash
```

Usuarios y Grupos

Está formada por 7 partes.

1) nombre del usuario
2) contraseña si aparece un x en ese campo indica que la contraseña en otro lugar
3) id de usuario (uid)
4) id de grupo (gid)
5) descripción
6) directorio de inicio
7) shell predeterminada

Las contraseñas de los usuarios están encriptadas y se almacenan en el archivo **/etc /shadow.**



1) Nombre de usuario
2) Contraseña cifrada
3) Fecha de último cambio
4) Días antes de cambio de contraseña
5) Días después de cambio de contraseña
6) Días antes de advertencia
7) Días de inactividad permitidos
8) Fecha de expiración de cuenta
9) Campo reservado

El usuario root se representa en el terminal con # y los no root con **$.**

Grupos de usuarios

Los grupos de usuarios en Unix se utilizan para administrar los permisos de los usuarios de una manera más fácil.

Usuarios y Grupos

Todos los usuarios pertenecen a un grupo de usuario, este se denomina **grupo primario**;
Si el usuario pertenece a más grupos, estos se denominan **grupos secundarios.**

Los grupos pueden contener varios usuarios, pero solo podrán contener usuarios.
Estos se denominan mediante **gid.**
La asignación de estos parte desde el 1000 para los grupos creados por el usuario, mientras que los menores de 100 se reservan para grupos especiales del sistema.

Grupos predeterminados

Grupos	Descripción
adm	Grupo de administración que permite accesos a archivos de registro y comandos como *sudo* y *su*
users	Grupo de usuarios estándar
nobody	Sin privilegios
root	Administración sin restricciones sobre todo el sistema
tty	Aporta privilegios sobre algunos dispositivos, como /dev/tty
lpadmin	Confiere privilegios sobre dispositivos de puerto paralelo

Administración(comandos) de grupos y usuarios

Crear usuarios	**useradd [opciones] nombre**	-**g** : grupo principal -**d** : carpeta home del usuario -**m** :Crear carpeta home -**s** :Interprete de comandos
Establecer contraseña	**passwd nombre**	
Modificación de usuarios	**usermod[opciones] nuevo nombre**	-**g** : grupo principal -**d** : carpeta home del usuario -**m** :Crear carpeta home -**s** :Interprete de comandos
Eliminar usuario	**userdel -r usuario**	
Crear grupos	**groupadd nombre-grupo**	

Usuarios y Grupos

Modificacion de grupos	**groupmod -g nuevo-gid -n nuevonombre nombregrupo**	
Añadir usuario a grupo	**adduser usuario grupo**	
Quitar usuarios de un grupo	**deluser usuario grupo**	
Modificar propietario	**chown[ops]nuevoPropietario fichero**	-**R** :aplicar cambios a contenido de los dirs -**h** :afecta al enlace simbólico
Modificar el grupo de un archivo	**chgrp [ops] nuevo_Grupo**	-**R** :afecta al contenido de los dirs
Modificar contraseña	**passwd [ops] contraseñanueva**	**d** : deja en blanco la contraseña **e** : hace expirar la passwd **i** : establece dias de inactividad despues de que expire la passwd **l** :bloquea la cuenta de usuario **u** :desbloquea la cuenta **x** :establece tiempo para cambiar la passwd **w** :antelacion para avisar de caducidad de la passwd
Modificar permisos	**chmod[ops] permisos nuevos**	-**R**: Opción recursiva para un directorio

Modificación de permisos

Octal
Administrar los permisos mediante números
Las equivalencias serían

- r(lectura) vale 4
- w (escritura) vale 2
- x(ejecución) vale 1

Simbólica
chmod [destinatarios] [tipo de mod] [permiso] archivo

Destinatarios

- **u** : propietario
- **g** : grupo
- **o** : otros
- **a** :t odos
-

Usuarios y Grupos

Tipo de modificación

- **+** : se añaden a los permisos actuales
- **=** : se establecen los nuevos
- **-** : se restan al valor actual

Permisos

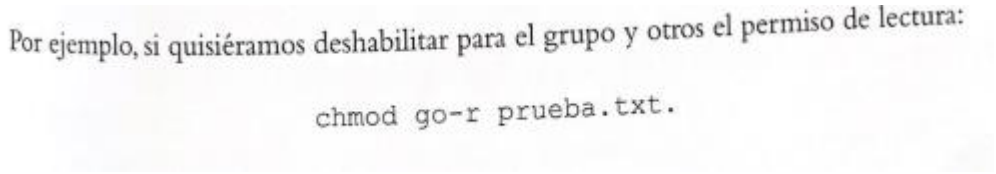
- **r** : lectura
- **w** : escritura
- **x** : ejecución
- **s** : set-uid/set-gid
- **t** : sticky-bit

Ejemplo:

- permisos = archivo
d permisos = directorio

chmod u+rw g+r
chmod u+rw g+r o+rw
chmod g+rx o+rwx
chmod u+rwx g+r

chmod 640
chmod 646
chmod 057
chmod 740


Por ejemplo, si quisiéramos deshabilitar para el grupo y otros el permiso de lectura:

```
chmod go-r prueba.txt.
```

---

grep es un comando de línea de comandos utilizado en sistemas operativos basados en Unix y Linux. Su función es buscar patrones de texto dentro de uno o varios archivos.

La sintaxis básica del comando grep es la siguiente:

grep [opciones] PATRÓN [ARCHIVO]

Donde:

- Opciones: son argumentos que modifican el comportamiento del comando. Algunas opciones comunes son -i (ignora mayúsculas y minúsculas), -r (busca de forma recursiva en subdirectorios) y -n (muestra los números de línea).

- PATRÓN: es el texto que se desea buscar. Puede ser una palabra, una cadena de caracteres o una expresión regular.

- ARCHIVO: es el archivo en el que se desea buscar. Si no se especifica ningún archivo, grep buscará en la entrada estándar.

Algunos ejemplos de uso de grep son:

Buscar una palabra en un archivo:
grep palabra archivo.txt

Buscar una palabra en varios archivos:
grep palabra archivo1.txt archivo2.txt
Buscar una palabra en todos los archivos de un directorio (de forma recursiva):
grep -r palabra directorio/
Buscar una palabra ignorando mayúsculas y minúsculas:
grep -i palabra archivo.txt

---

find es un comando de línea de comandos que se utiliza en sistemas operativos basados en Unix y Linux para buscar archivos

find [ruta] -name [patrón]: Busca archivos y directorios por nombre. ruta es la ubicación donde se desea buscar y patrón es el nombre o patrón de nombres que se desea buscar.

find [ruta] -type [tipo]: Busca archivos y directorios por tipo. tipo puede ser f para archivos regulares, d para directorios, l para enlaces simbólicos, entre otros.

find [ruta] -mtime [días]: Busca archivos modificados hace días días. ruta es la ubicación donde se desea buscar.

find [ruta] -size [tamaño]: Busca archivos por tamaño. tamaño puede ser n para archivos de exactamente n bloques de tamaño, n+c para archivos de más de n bloques de tamaño, -n para archivos de menos de n bloques de tamaño, entre otros.

find [ruta] -exec [comando] {} \;: Ejecuta un comando para cada archivo o directorio encontrado. comando es el comando que se desea ejecutar, y {} es el marcador de posición para el archivo o directorio encontrado.

El comando **umask** en Ubuntu es utilizado para establecer los permisos predeterminados de los archivos y directorios creados por un usuario. El valor de umask se resta de los permisos máximos que se establecen en un archivo o directorio. Por lo tanto, cuanto mayor sea el valor de umask, menor serán los permisos predeterminados que se aplicarán a los nuevos archivos y directorios creados.

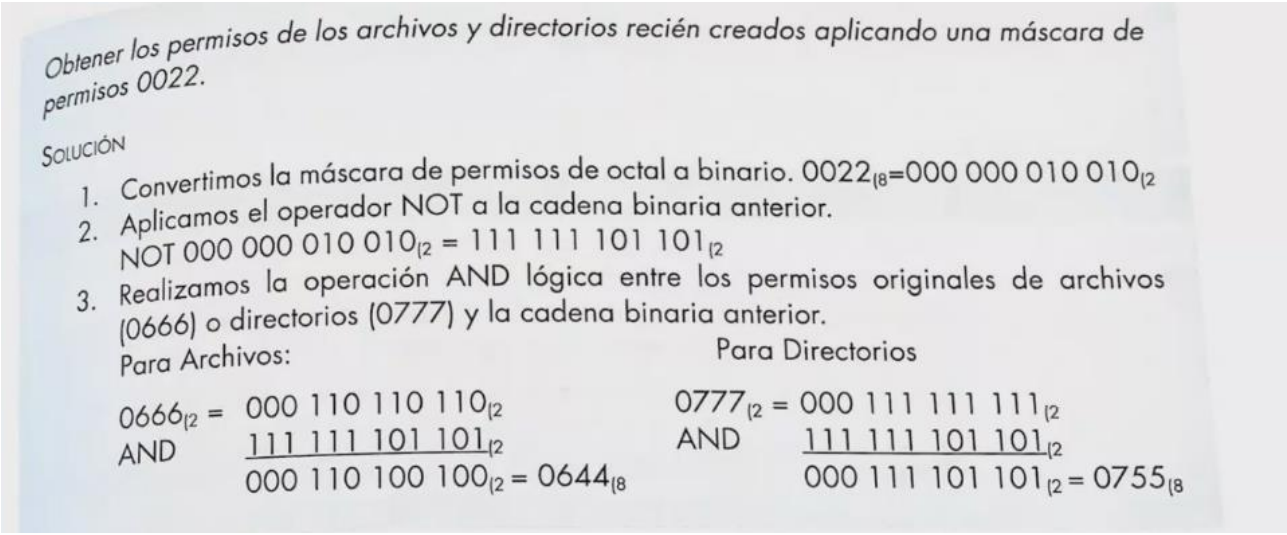
El valor de umask se representa generalmente en octal (base 8) y se puede establecer utilizando el comando umask seguido del valor de umask deseado. Por ejemplo, si se desea establecer un umask de 022, se puede utilizar el siguiente comando:

Usuarios y Grupos

umask 022

Esto establecerá permisos predeterminados para archivos nuevos de 644 (rw-r--r--) y para directorios nuevos de 755 (rwxr-xr-x).

El valor predeterminado de umask en Ubuntu es 002, lo que significa que los nuevos archivos tendrán permisos de lectura y escritura para el propietario y el grupo, y permisos de lectura para otros usuarios, mientras que los nuevos directorios tendrán permisos de lectura, escritura y ejecución para el propietario y el grupo, y permisos de lectura y ejecución para otros usuarios.



Obtener los permisos de los archivos y directorios recién creados aplicando una máscara de permisos 0022.

SOLUCIÓN

1. Convertimos la máscara de permisos de octal a binario. $0022_{(8}=000\ 000\ 010\ 010_{(2}$
2. Aplicamos el operador NOT a la cadena binaria anterior.
   NOT $000\ 000\ 010\ 010_{(2} = 111\ 111\ 101\ 101_{(2}$
3. Realizamos la operación AND lógica entre los permisos originales de archivos (0666) o directorios (0777) y la cadena binaria anterior.

Para Archivos:

$0666_{(2} = 000\ 110\ 110\ 110_{(2}$
AND $111\ 111\ 101\ 101_{(2}$
$000\ 110\ 100\ 100_{(2} = 0644_{(8}$

Para Directorios

$0777_{(2} = 000\ 111\ 111\ 111_{(2}$
AND $111\ 111\ 101\ 101_{(2}$
$000\ 111\ 101\ 101_{(2} = 0755_{(8}$

0 + 0 = 0
1 + 0 = 0
0 + 1 = 0
1 + 1 = 1