

8.- Administración de usuarios

8.1.- Servicio NIS y NFS

Antes de comenzar con el apartado sobre la administración de usuarios ha de tenerse en cuenta estos dos servicios dada su importancia.

Servicio NIS

NIS es un servicio para centralizar nombres de usuarios, claves e información de grupos en el servidor facilitando la administración de usuarios. Si además de NIS se usa NFS para montar el directorio **/home** del servidor en cada cliente, puede centralizarse también la información de todos los usuarios en el servidor.

Con estos servicios puede centralizarse información de usuarios y claves en el servidor

NIS de forma análoga a DNS opera sobre un grupo de computadores (dominio) y mantiene bases de datos (mapas) centralizadas en un servidor maestro, que pueden ser consultadas por los clientes. Para disminuir carga podrían ponerse servidores esclavos que repliquen la información del servidor maestro.

Para usar NIS debe escoger un nombre de dominio NIS (puede ser diferente al dominio DNS) y usarlo en los computadores clientes y en el servidor.

Puede comenzar instalando el paquete NIS tanto en clientes como servidor, al instalarlo podrá dar el dominio NIS (o puede editarlo en `/etc/defaultdomain`). En todos los computadores debe modificar el archivo `/etc/nsswitch` para cambiar el orden de búsqueda de usuarios, grupos y *shadow*. También debe agregar algunas líneas al final de los archivos `/etc/passwd`, `/etc/group` y `/etc/shadow`, tarea que puede hacer con los siguientes comandos:

```
echo "+::::::" >> /etc/passwd
echo "+:::" >> /etc/group
echo "+:::::::" >> /etc/shadow
```

Que agregan líneas con un "+" y tantos ":" como separadores hay en los respectivos archivos. En el servidor los usuarios y grupos que estén después de estas marcas no serán compartidos por NIS.

En el servidor debe configurar NIS de la siguiente forma:

1. Edite `/etc/init.d/nis`, asegurándose de dejar `NISSERVER=master`.
2. Reinicie el servicio NIS con **`/etc/init.d/nis restart`**
3. Edite el archivo `/var/yp/Makefile` y cambie la regla `all`: para que incluya también `shadow`.
4. Ejecute **`/usr/lib/yp/ypinit -m`**.

Una vez NIS esté funcionando en clientes y servidor, puede agregar, eliminar o modificar usuarios y grupos con los comandos usuales y después de cada modificación, para que el cambio sea notado por NIS, debe pasar al directorio `/var/yp/` y ejecutar **`make`**.

Para centralizar la información de todos los usuarios en el servidor puede usar NFS una vez NIS funcione bien. Para lograrlo se debe hacer la administración de usuario siempre en el servidor (por ejemplo agregar nuevos usuarios sólo desde el servidor) para que los directorios queden allí; por otra parte debe montar el directorio `/home` del servidor en todos los clientes. Para centralizar la cola de correo en el servidor debe montar el directorio `/var/mail` del servidor en los clientes. De esta forma el archivo `/etc/fstab` de cada cliente debe incluir:

```
servidor.micolegio.edu.co:/home /home nfs rw 0 0
```

```
servidor.micolegio.edu.co:/var/mail /var/mail nfs rw 0 0
```

y el archivo `/etc/exports` del servidor debe tener las líneas apropiadas para exportar `/home` y `/var/mail`.

Servicio NFS

Este servicio permite compartir directorios de un servidor en uno o más clientes.

Como se describe en el RFC 1813, el protocolo NFS permite acceder de forma transparente sistemas de archivos compartidos que están en máquinas remotas. Hay muchas posibilidades para usar este servicio, nuestra plataforma de referencia lo aprovecha para distribuir información de usuarios (directorio `/home` del servidor), las colas de correo (`/var/mail`) y los programas y documentos disponibles en el servidor (directorio `/usr`). Así mismo permite aprovechar el espacio de sobra de cada cliente (directorio `/aux`).

Archivo de configuración de NFS en un servidor, donde se especifica que directorios son exportables.

Al igual que otros servicios, NFS cuenta con un cliente y un servidor. El servidor NFS permite exportar directorios del computador en el que corre a computadores donde se ejecute el cliente, mientras estos últimos tengan permiso para importar tales directorios. Los directorios que se exportan, así como las restricciones sobre los clientes que pueden importarlos se especifican en el archivo `/etc/exports`. Por ejemplo el siguiente es el archivo `/etc/exports` del servidor de nuestra plataforma de referencia:

```
/usr *.micolegio.edu.co(ro,no_root_squash)
/home *.micolegio.edu.co(rw,no_root_squash)
/var/mail *.micolegio.edu.co(rw,no_root_squash)
```

Este archivo especifica que pueden exportarse con permiso de lectura y escritura los directorios `/home`, `/var/mail`. Puede exportar con permiso de sólo lectura (`ro`) el directorio `/usr`. Todos estos directorios pueden ser importados por máquinas con nombres de la forma `x.micolegio.edu.co`. La opción `no_root_squash` indica que los archivos de usuario y grupo `root` exportados del servidor sean tratados como si fueran del usuario y grupo `root` en los clientes.

En nuestra plataforma de referencia tanto cliente NFS como servidor NFS deben instalarse en todos los computadores (porque los computadores clientes exportarán el espacio que resta de su partición `aux` al servidor). El archivo `/etc/exports` de cada cliente debe ser algo como:

```
/aux *.micolegio.edu.co(rw,no_root_squash)
```

Para instalar el servidor y el cliente NFS en Debian 2.2 basta que instale los paquetes `nfs-common` y `nfs-server`, siguiendo el procedimiento usual. Como NFS depende de RPC, asegúrese también de dar acceso a las máquinas de su dominio con portmap y que esté operando. Dado que portmap es manejado con **tcpd** este acceso se da o restringe modificando los archivos `/etc/hosts.allow` y `/etc/hosts.deny`. Por ejemplo el archivo `/etc/hosts.allow` debe tener una línea como:

```
portmap: .micolegio.edu.co
```

Puede comprobar que portmap está corriendo buscándolo entre los procesos (**ps ax | grep "[p]ortmap"**) o revisando los programas que están registrados para usar RPC con `pmap_dump`.

Una vez esté corriendo el servidor y el cliente NFS en todas las máquinas, puede montar los directorios exportados por el servidor en cada cliente, por ejemplo con algo como:

```
mount -t nfs servidor.micolegio.edu.co:/usr /opt
```

para montar el directorio `/usr` del servidor como el directorio `/opt` de cada cliente. Mejor aún, puede editar el archivo `/etc/fstab` para que cada vez que cada máquina inicie monte automáticamente ese directorio. Por ejemplo podría agregar la siguiente línea al archivo `/etc/fstab` de un cliente:

```
servidor.micolegio.edu.co:/usr /opt nfs ro 0 0
```

En el servidor puede agregar al archivo `/etc/fstab`, líneas de la forma "`cliente:/aux /mnt/auxn nfs rw 0 0`" para montar en `/mnt/auxn` el directorio `/aux` de cada cliente. Para comprobar los directorios que ha montado con NIS puede emplear **mount**.

Mientras no configure el servicio NIS, recomendamos no montar `/home` ni `/var/mail` del servidor en los clientes.

8.2.- Notas sobre la administración de usuarios

El objetivo de los usuarios, grupos y permisos en Unix es brindar privacidad y organización permitiendo también compartir información cuando así se desea.

Con respecto a usuarios el administrador puede crear, eliminar o modificar información de cuentas y grupos. También puede configurar detalles de los programas que permiten iniciar sesiones y prevenir fallas de seguridad. Si aún no lo ha hecho, antes de consultar esta sección recomendamos estudiar la visión que un usuario tiene del sistema de usuarios y grupos.

En una red con NIS la información de cuentas y grupos está centralizada en el servidor. Desde este debe hacerse la administración con los programas y archivos presentados en esta sección y después de cada cambio debe reconfigurarse NIS como se explicará posteriormente.

Usuarios

Los siguientes programas permiten realizar operaciones relacionadas con los usuarios:

su [*usuario*]

Permite entrar a una sesión como un usuario diferente, si no se especifica un usuario como primer parámetro, **su** cambia al usuario root. Desde una cuenta de usuario pedirá la clave del nuevo usuario, e iniciará el intérprete de comandos que el usuario haya configurado. Si se emplea la opción **-c** comando el comando se ejecutará.

Si desea ejecutar un intérprete de comandos diferente al configurado por el usuario emplee la opción **-s** *intérprete*, donde *intérprete* debe ser la ruta completa del intérprete de comandos que además debe estar listada en el archivo `/etc/shells`.

su al igual que **login** emplea los servicios de la librería PAM (Pluggable authentication modules), así que puede configurar varios detalles

relacionados con seguridad de **su** en el archivo `/etc/pam.d/su` por ejemplo para restringir el uso de este comando.

passwd [*usuario*]

Permite cambiar la clave del usuario especificado (sólo root puede especificar un usuario). Si no se especifica un usuario permite cambiar la clave de la cuenta desde la cual se ejecuta. Por defecto un usuario podrá cambiar su clave cuando él/ella lo desee, aunque puede implementarse una política de expiración de claves. La política de un usuario puede examinarse con la opción `-S` que presenta: estado de la cuenta (L bloqueada, NP sin clave, P con clave utilizable), fecha del último cambio de clave, tiempos mínimo y máximo para cambiar clave, tiempo de avisos y tiempo para desactivación. Puede fijarse la política con las siguientes opciones:

`-x días` para especificar el máximo de días antes de que un usuario deba cambiar su clave.

`-w días` para indicar con cuantos días de anterioridad a la expiración de la clave el sistema debe empezar a enviar correos recordando el cambio;

`-i días` para deshabilitar una cuenta cuya clave no haya sido cambiado en los días especificados. Una cuenta puede bloquearse para impedir que pueda usarse con el programa login.

Pueden bloquear y desbloquear cuentas con las opciones `-u` (de unlock) y `-l` respectivamente.

chage *usuario*

Cambia la información sobre el envejecimiento de la clave de un usuario, cuando se están usando claves shadow.

Para cambiar el mínimo de días entre cambios se usa la opción `-m días` (0 indica que puede cambiarse siempre), `-M días` para indicar máximo de

días antes de la expiración de la clave, **-d** *días* para establecer fecha del último cambio de clave (contada en días a partir de 1/Ene/1975), **-E** *fecha* fecha en la cual la cuenta expirar (puede especificarse como una fecha mm/dd/aaaa o contada en días a partir de 1/Ene/1975), **-I** *días* establece cantidad de días de inactividad antes de bloquear una cuenta después de la expiración de la clave, **-W** *días* cantidad de días de preaviso antes de la caducidad de la clave.

adduser login

Permite agregar un usuario con el login dado, opcionalmente indicando el directorio de trabajo (opción *home*) que de no existir será creado, un número que identificará al usuario de forma única (opción *uid*), el grupo principal al que pertenecerá (opción *ingroup grupo*), el intérprete de comandos por defecto (opción *shell nombre*) y otros datos del usuario con la opción *gecos "datos"* (los datos se separan con comas y por defecto son: nombre, número de cuarto, teléfono del trabajo y teléfono de la casa).

A menos que se especifique *disabled-login* o *disabled-password* pedirá clave inmediatamente después de crear la cuenta (*disabled-login* bloquea la cuenta hasta que se asigne una clave, *disabled-password* no bloquea la cuenta pero asigna una clave no válida, el usuario podría entrar por ejemplo con RSA ssh).

Las operaciones que **adduser** realiza se configuran en el archivo */etc/adduser.conf*. Por defecto creará cuentas de usuarios en el directorio */home* y copiará en los nuevos directorios los archivos del directorio */etc/skel* (e.g. *.bash_profile*), pondrá como intérprete de comandos por defecto ***/usr/bin/bash*** y asignará un número de usuario y un grupo nuevo a cada usuario.

Normalmente después para agregar un usuario debe especificar la clave que tendrá, si prefiere crear una cuenta inicialmente sin clave emplee la opción `disabled-password` (antes de poder emplear la cuenta debe establecer la clave con **passwd**).

chfn [*login*]

Para cambiar la información GECOS de un usuario (si no se especifica un login se cambiará la información del usuario que emplee el programa). Como opciones recibe **-f** nombre, **-r** cuarto, **-w** teléfono_trabajo, **-h** teléfono casa y **-o** otros_datos. Nuestra sugerencia es emplear en lugar de cuarto el grado y en lugar del teléfono del trabajo la dirección de la casa. Estos datos no deben contener los caracteres `'`, `'`; ni `'=`.

Los datos que no se especifiquen en la línea de comandos serán solicitados interactivamente. **chfn** también será llamado por **passwd** si se emplea la opción **-f**.

chsh [*login*]

Para cambiar el intérprete de comandos de un usuario (si no se especifica un login se cambiará el intérprete del usuario que emplee el programa). Como opción recibe el nombre del intérprete, el cual debe estar listado en el archivo `/etc/shells`. Un usuario que emplee un intérprete de comandos restringido (`/bin/rsh`) no puede cambiar su shell. **chsh** también será llamado por **passwd** si se emplea la opción **-s**.

deluser *login*

Para eliminar una cuenta Por defecto no elimina el directorio personal ni la cola de correos, puede indicarse que se borren estos directorios con la opción `remove-home` y puede indicarse que se busquen y eliminen todos los archivos del usuario (en los demás directorios) con la opción `-remove-all-files`. Con la opción `backup` creará un archivo comprimido con los datos del usuario en el directorio de trabajo con nombre `login.tar.gz`. El

comportamiento por defecto de este comando puede configurarse en el archivo `/etc/default/passwd`.

La información sobre usuarios se mantiene en el archivo que todos los usuarios pueden leer: `/etc/passwd`. Cada línea de este archivo tiene información de un usuario separada con el carácter ':'. De cada usuario mantiene:

login

Clave o un carácter de control. En sistemas Unix las claves antes de ser almacenadas en este archivo (para su posterior comparación) son convertidas a una secuencia de letras y números con un algoritmo (bien DES o bien MD5), cada vez que un usuario desea ingresar al sistema la clave que teclea se transforma con ese algoritmo y se compara con la almacenada para dar acceso sólo si son iguales. Por las características de DES y MD5 es muy difícil recuperar la clave original partiendo de la información almacenada en `/etc/passwd` así que una persona con acceso a este archivo no podrá conocer fácilmente las claves de los usuarios.

Sin embargo es mejor emplear el sistema de claves shadow, que mantiene las claves en un archivo aparte que sólo pueda ser leído por el administrador: `/etc/shadow`, las cuentas que empleen este mecanismo tendrán un carácter 'x' en lugar de clave.

Tanto en `/etc/passwd` como en `/etc/shadow` en lugar de clave transformada puede aparecer el carácter '*' para indicar que la cuenta tiene clave deshabilitada (opción `disabled-password` de `adduser`), el usuario podría ingresar con RSA ssh.

En lugar de la clave también puede aparecer el carácter '!' para indicar que la cuenta está bloqueada (opción `disabled-login` de **adduser**), en este caso el usuario no podrá entrar con **login** ni con gdm ni con RSA ssh, pero si con **su** y se ejecutarán procesos del usuarios iniciados por **cron** o **at** está bloqueada (el usuario no podrá entrar con login o gdm pero si con rlogin o **su** y se ejecutarán procesos del usuarios iniciados por **cron** o **at**).

- GID, es decir número que identifica al grupo principal del usuario.

- información GECOS , los datos se separan entre si con comas.
- directorio personal
- intérprete de comandos

En el archivo `/etc/shadow` hay una línea por cada usuario con los siguientes datos separados por ':':

- Login
- Clave transformada
- Fecha del último cambio de la clave (contada en días a partir del Enero 1 de 1975).
- Días por esperar antes de que la clave pueda ser cambiada.
- Máximo de días antes de exigir un cambio de clave.
- Cantidad de días de preaviso antes de expiración de clave.
- Cantidad de días entre expiración de clave y bloqueo de cuenta.
- Fecha desde la cual la cuenta está deshabilitada (contada en días desde Enero 1 de 1975).
- Campo reservado.

Aunque puede editar manualmente `/etc/passwd` y `/etc/shadow` es recomendable que emplee los programas presentados en esta sección.

Los GID y UID reservados en linux están en los archivos

`/usr/share/base-passwd/group.master` y `/usr/share/base-passwd/passwd.master`

si algún programa o administrador erradamente asigna alguno de estos números puede emplear `update-passwd` para reasignar los originales.

Grupos

El objetivo de los grupos es dar o restringir permisos sobre algunos archivos a ciertos usuarios. Por ejemplo un archivo `reporte.txt` que pertenezca al grupo profesores, que tenga permiso de lectura para el grupo y no para otros usuarios (si por ejemplo se estableció con `chmod ug=rw reporte.txt`), podrá ser leído únicamente por el dueño y por usuarios que pertenezcan al grupo profesores.

Cada usuario tiene un grupo principal (puede especificarse durante la creación con la opción `gid GID` o `ingroup grupo` de **adduser**), puede pertenecer a diversos grupos y si conoce la clave de algún grupo con clave puede volverse miembro durante una sesión. Los programas relacionados con grupos son:

adduser *usuario grupo*

Para agregar un usuario a un grupo. En Linux algunos dispositivos pertenecen a ciertos grupos, de forma que es indispensable agregarlos como grupos secundarios de los usuarios que los requieran:

audio	Permite acceder a dispositivos de sonido.
lp	Permite acceder a los puertos locales de impresión.
floppy	Para acceder a la(s) unidad(es) de disquette.
tape, cdrom	Ambos son requeridos para acceder al CDRom.
dialout	Para acceder a modems.
disk	Cuando se requiere acceder a discos a bajo nivel.
kmem	Para acceder de forma privilegiada la memoria.
tty	Para acceder de forma privilegiada a la consola.

groups

Un usuario puede ver los grupos a los que pertenece con este programa.

newgrp [grupo]

Para cambiarse a un grupo con clave. Si no se especifica grupo alguno se cambiará al grupo principal del usuario.

passwd -g grupo

Para cambiar la clave de un grupo. Para quitar la clave de un grupo se emplea **passwd -g -r grupo** ---los programas **newgrp** y **sg** no permiten cambiarse a un grupo sin clave.

gpasswd grupo

Para administrar grupos con clave, puede ser usado por el administrador del sistema y por el administrador de un grupo con clave. Con la opción `-A login` el administrador del sistema puede agregar un administrador de grupo a un grupo, con la opción `-M login` puede retirarse la administración de un grupo a un usuario, con la opción `-r` puede quitarse la clave a un grupo con clave y con la opción `-R` puede inhibir el acceso con **newgrp** a un grupo con clave. Un administrador de grupo puede agregar y eliminar usuarios del grupo con las opciones `-a login` y `-d login` respectivamente.

addgroup *nombre*

Permite agregar un grupo con el nombre dado. Con la opción `gid ID` puede especificarse el número que identificará al grupo, número acorde con el archivo `/etc/adduser.conf`.

groupdel *group*

Permite eliminar un grupo. Sólo pueden eliminarse grupos que no sean el grupo principal de algún usuario.

groupmod *grupo*

Permite modificar información de un grupo. Las opciones posibles son: `-g GID` para cambiar el número que identifica al grupo (ver convenciones en descripción de **addgroup**) y `-n nombre` para cambiar el nombre del grupo. El número que identifica al grupo debe ser único, excepto si se emplea la opción `-o` (para crear grupos alias, aunque el sistema de archivos no necesariamente presentará el alias como grupo dueño).

grpck

Para verificar la información de grupos en `/etc/group` y `/etc/gshadow`. Con la opción `-r` abre estos archivos en modo de sólo lectura.

La información de grupos se consigna en `/etc/groups`, cada línea tiene los siguientes datos de un grupo separados uno de otro con el carácter `:`

- Nombre del grupo
- Clave del grupo transformada con DES o MD5. Si el grupo tiene clave shadow en este archivo aparecerá el caracter 'x' y la clave transformada estará en otro archivo (por defecto /etc/gshadow).
- GID
- Lista d usuarios del grupo separados con comas.

No es recomendable editar directamente estos archivos, sino más bien emplear los programas presentados en esta sección.

8.3.- Inicio de sesiones en consolas virtuales

Una sesión iniciada desde una consola virtual o desde una conexión remota (via **telnet**, **rsh** o **ssh**) es atendida inicialmente por el programa **getty**.

El mensaje que presenta **getty** se configura en el archivo /etc/issue y puede contener algunas secuencias especiales como:

\d que corresponde a la fecha.

\s al nombre del sistema operativo

\l al número de la consola virtual (línea tty)

\m al tipo de procesador

\n al nombre de la máquina

\u cantidad de usuarios conectados.

Cuando un usuario teclea su login, **getty** pasa el control al programa **login**. El programa **login** por intermedio de la librería PAM espera la clave del usuario y la válida, cuando el usuario da la clave correcta verifica que el acceso para ese usuario a la hora del ingreso sea posible y entonces inicializa algunas variables de ambiente, muestra algunos mensajes (por defecto la fecha de la última conexión y el contenido del archivo /etc/motd) e inicia un intérprete de comandos (el que está configurado para el usuario en /etc/passwd).

Las acciones que **login** realiza pueden configurarse en los archivos /etc/login.def y /etc/pam.d/login, las consolas desde las cuales puede ingresar el usuario root se configuran en /etc/securetty, otras restricciones de seguridad pueden configurarse en los archivos del directorio /etc/security.

8.4.- Ejercicios

1. Los números UID y GID del usuario root son fijos, investigue en su sistema cuales son.

Solución

UID=0 y GID=0. Son menores a 100 lo que indica que deben ser fijos del sistema.

2. En el directorio tarea1 se quiere que todos los miembros del grupo estudiantes puedan escribir, pero que un miembro de ese grupo no pueda borrar o renombrar archivos de otros, ¿cómo puede lograrse? si además se quiere que no puedan ver o modificar el contenido de archivos de otros miembros del mismo grupo que se requiere?

Solución

```
chgrp estudiantes tarea1;  
chmod o+t tarea1
```

Para la segunda parte se requiere que cada archivo no conceda permiso de lectura ni escritura al grupo ni a otros.

3. Para transformar una clave con el algoritmo DES puede emplear el siguiente script escrito en lenguaje Perl.

Solución

```
#!/usr/bin/perl  
$sal=join " ", ('.', '/', 0..9, 'A'..'Z', 'a'..'z')[rand 64, rand 64];  
print crypt($ARGV[0], $sal);  
print "\n";
```

Si el nombre del script es **enc.pl** y le da permiso de ejecución, para transformar la clave "vida" bastaría ejecutar **enc.pl vida**.

Emplee este script para transformar una clave, después edite /etc/passwd o /etc/shadow agregue la nueva clave transformada a una cuenta de prueba y finalmente compruebe que la nueva clave funciona entrando a la cuenta de prueba. Nota: Si desea experimentar con MD5 en lugar de DES debe cambiar la "sal", remplazando la línea con la función **crypt** por **print crypt(\$ARGV[0],"\\$1\\$\$sal");**

"enc.pl vida" (con MD5) da por ejemplo "\$1\$wv\$mOwf63L.QvbJ.f7U362Os1" que puede ponerse bien en el campo para la clave de /etc/passwd o bien si las claves shadow están activas, dejar 'x' en /etc/passwd y remplazar la clave en /etc/shadow.

4. Cree un usuario en el grupo users y agréguelo a grupos que le permitan acceder a la impresora local, a dispositivos de audio y a la unidad de disquette. Después pase a la cuenta del nuevo usuario y compruebe que pueda usar disquettes. Finalmente elimine el usuario creado.

Solución

```
adduser ingroup users gloria
adduser gloria lpr
adduser gloria audio
adduser gloria floppy
su - gloria
mdir
exit
deluser remove-home gloria
```

5. Nuestra plataforma de referencia sugiere 3 grupos básicos: profesores, estudiantes y administración. Considere ventajas y desventajas de esta política ¿Qué usuarios deberían tener más de un grupo? ¿Qué grupos podrían tener clave, quienes administrarían tales grupos y quienes serían los usuarios?

Solución

Los grupos básicos no tendrían clave: profesores, estudiantes y administración (podrían crearse grupos para otros miembros de la comunidad como antiguos alumnos o padres). Los estudiantes pueden estar sólo en el grupo de estudiantes, los profesores pueden tener como segundo grupo estudiantes, los usuarios de la parte administrativa podrían tener como grupo principal administración y como grupos secundarios profesores y estudiantes.

En principio la información que cree un usuario no debe ser visible a su grupo. Podrían haber grupos con clave para grupos liderados por un profesor, administrador o estudiante que requieran manejar información separada (con un poco de instrucción los líderes podrían ser los administradores de grupo).

6. Cree los grupos que decidió en el punto anterior y usuarios de prueba (de forma que al menos un usuario de prueba esté en dos grupos).

Solución

```
addgroup gid 1100 estudiantes;  
addgroup gid 1101 profesores;  
addgroup gid 1102 admin;  
adduser ingroup estudiantes esperanza;  
adduser ingroup profesores johannes;  
adduser ingroup tomas;  
adduser estudiantes johanes;  
adduser estudiantes tomas;  
adduser profesores tomas
```

7. ¿Qué cambios puede realizar en `/etc/adduser.conf` para facilitar la implementación de la política descrita en los ejercicios anteriores?

Solución

Suponiendo que los grupos son estudiantes (GID=1100), profesores (GID=1101), cuerpo administrativo (GID=1102) `adduser.conf` puede ser como el que viene por defecto con los siguientes cambios:

`USERGROUPS=no`

USERS_GID=1100

Así por defecto todo usuario nuevo sería estudiante (para agregar profesores y administradores se usaría la opción ingroup de **adduser**). Entre las opciones por defecto de ese archivo que puede ser mejor conservar están: bash como intérprete de comandos por defecto, como directorio para usuarios /home .

8.5.- Ayudas al Profesor

1. Piense una máscara de permisos apropiada para todos los usuarios. Describa como la aplica empleando **umask** y los cambios que debe realizar para establecer tal mascara por defecto para todos los usuarios.

Como se desea que por defecto los usuarios de unos grupos no puedan ver información de usuarios del mismo grupo: **umask u=rw,g=,o=**. Debe agregarse tal orden en /etc/profile y en los archivos de sesiones de **gdm** en el directorio /etc/gdm/Session.

2. Haga los cambios apropiados en su sistema, para que todo directorio creado para nuevos usuarios tenga un archivo ayuda.txt donde los usuarios podrían escribir sus propias notas para emplear bien el sistema, y un mecanismo que le recuerde a los usuarios la existencia de tal archivo. Inicialmente ese archivo podía tener un mensaje de bienvenida y/o instrucciones para comenzar a usar bien el sistema.

Crear el archivo en etc/skel (como parte del contenido puede recordarse a los usuarios actualizar la información personal con **chfn**). En /etc/skel/.bashrc puede agregarse algo como:

```
echo "Hay ayuda que puede completar en el archivo ayuda.txt"
```

3. Haga una lista de chequeo de detalles que deba tener en cuenta para prevenir que alguien entre a cuentas que no le pertenecen (especialmente como evitar que alguien pueda entrar a la cuenta root).

Evitar entrada a la cuenta root desde el prompt de arranque. Evitar en lo posible emplear los bits SUID y GUID con usuario o grupo root. Emplear claves shadow con MD5. Educar a los usuarios en este tema, buscando que elijan buenas claves y ayuden a cuidar y construir la red (emplear para la cuenta root una muy buena clave conocida sólo por el administrador). Emplear cracklib para evitar uso de claves simples.

4. Configure gdm para que en vez de presentar el logo típico presente el logo de su institución educativa.

Editar en /etc/gdm/gdm.conf la línea:

logo=/usr/share/pixmaps/gnome-logo-large.png