

Examen 107 - Tareas Administrativas

Este examen cubre la gestión de usuarios y grupos, la automatización de tareas y la configuración de localización del sistema.

107.1 Gestionar cuentas de usuario y grupo y archivos relacionados

Teoría

En un sistema multiusuario como Linux, los usuarios y grupos son los mecanismos fundamentales para controlar el acceso a los recursos del sistema (archivos, procesos, etc.). Cada usuario tiene una cuenta, identificada por un nombre de usuario y un ID numérico (UID). Los usuarios se organizan en grupos, identificados por un nombre de grupo y un ID numérico (GID).

Conceptos Clave:

1. **Usuarios (Users):** Representan individuos o servicios. Cada usuario tiene un UID único en el sistema local. El usuario `root` (UID 0) es el superusuario con privilegios ilimitados. Los UID del sistema (normalmente 1-999 o 1-499 dependiendo de la distribución) se usan para servicios y demonios, mientras que los UID de usuario interactivos comienzan a partir de 1000 (o 500).
2. **Grupos (Groups):** Son colecciones de usuarios. Los permisos sobre archivos y directorios se pueden asignar a grupos. Cada grupo tiene un GID único.
3. **Grupo Primario (Primary Group):** Cada usuario pertenece a un grupo primario. Este es el grupo que se asigna por defecto a los archivos y directorios que el usuario crea.
4. **Grupos Secundarios (Secondary Groups):** Un usuario puede ser miembro de grupos adicionales (secundarios). Esto otorga al usuario los permisos asignados a esos grupos sin cambiar su grupo primario.

Archivos de Configuración Clave (Requieren permisos de root para leer/modificar):

Estos archivos son la base de datos local de usuarios y grupos:

1. **/etc/passwd:** Contiene información básica sobre cada cuenta de usuario. Cada línea representa un usuario y tiene 7 campos separados por dos puntos (:):
 - Nombre de usuario.
 - x (indicador de que la contraseña está almacenada en `/etc/shadow`).
 - UID (User ID).
 - GID (Group ID del grupo primario).
 - Campo de comentarios/GECOS (información opcional como nombre completo).
 - Directorio personal (Home directory).
 - Shell de inicio de sesión (Login shell).
 - **Nota:** Este archivo es legible por todos los usuarios (`rwXr-Xr-X` o similar), pero la contraseña no está aquí por seguridad.

2. **/etc/shadow:** Contiene información segura sobre las cuentas de usuario, incluyendo contraseñas encriptadas, antigüedad de la contraseña y fechas de caducidad.
 - **¡Crucial!** Este archivo solo es legible por el usuario `root` (`rw-----`).
 - Cada línea tiene 9 campos: Nombre de usuario, contraseña encriptada, fecha del último cambio de contraseña, antigüedad mínima, antigüedad máxima, fecha de advertencia, fecha de caducidad de la cuenta, campo reservado, campo reservado.
3. **/etc/group:** Contiene información sobre los grupos. Cada línea representa un grupo y tiene 4 campos:
 - Nombre del grupo.
 - x (indicador de que la contraseña del grupo está en `/etc/gshadow`, aunque las contraseñas de grupo se usan poco).
 - GID (Group ID).
 - Lista de miembros secundarios del grupo (separados por comas). El miembro del grupo primario *no* aparece en esta lista.
 - **Nota:** Este archivo es legible por todos los usuarios.
4. **/etc/gshadow:** Contiene información segura sobre los grupos, incluyendo contraseñas de grupo y administradores del grupo. Similar a `/etc/shadow` pero para grupos.
 - **¡Crucial!** Este archivo solo es legible por el usuario `root`.

Comandos para Gestionar Usuarios y Grupos (Requieren privilegios de root - sudo):

Las distribuciones proporcionan comandos de alto nivel que modifican automáticamente los archivos `/etc/passwd`, `/etc/shadow`, `/etc/group` y `/etc/gshadow` de forma segura.

1. **useradd:** Crea una nueva cuenta de usuario.
 - `sudo useradd <nombre_usuario>`: Crea un usuario con valores por defecto.
 - **Diferencias Debian vs. Red Hat:**
 - **Debian/Ubuntu:** Por defecto, `useradd` *no* crea automáticamente el directorio personal del usuario ni establece una contraseña. Necesitas usar opciones o comandos adicionales. El grupo primario es un grupo con el mismo nombre que el usuario (User Private Group - UPG scheme).
 - **RHEL/CentOS/Fedora:** Por defecto, `useradd` *sí* crea el directorio personal (`/home/nombre_usuario`) y copia archivos de `/etc/skel`. El grupo primario es también un UPG.
 - **Opciones comunes:**
 - `-m`: Crea el directorio personal (si la distribución no lo hace por defecto).
 - `-d <directorio_home>`: Especifica el directorio personal.
 - `-s <shell>`: Especifica la shell de inicio de sesión (ej: `/bin/bash`, `/sbin/nologin`).
 - `-u <uid>`: Especifica el UID.
 - `-g <grupo_primario>`: Especifica el GID del grupo primario.

- **-G <lista_grupos_secundarios>**: Añade el usuario a grupos secundarios (lista separada por comas).
- **-c "Comentario"**: Añade información al campo GECOS.
- **-e <fecha_caducidad>**: Establece fecha de caducidad de la cuenta.
- **-f <dias_inactivo>**: Establece número de días tras caducar la contraseña para que la cuenta sea deshabilitada.

2. **userdel**: Elimina una cuenta de usuario.

- **sudo userdel <nombre_usuario>**: Elimina la cuenta, pero *no* su directorio personal ni su spool de correo.
- **sudo userdel -r <nombre_usuario>**: Elimina la cuenta y su directorio personal y spool de correo. **Esta es la opción más común.**

3. **usermod**: Modifica una cuenta de usuario existente.

- **sudo usermod [opciones] <nombre_usuario>**
- **Opciones comunes:**
 - **-d <nuevo_directorio_home> [-m]**: Cambia el directorio personal. Usar -m para mover el contenido del viejo al nuevo.
 - **-s <nueva_shell>**: Cambia la shell de inicio de sesión.
 - **-l <nuevo_nombre>**: Cambia el nombre de usuario (requiere que el usuario no esté logueado).
 - **-u <nuevo_uid>**: Cambia el UID (riesgoso si el usuario posee muchos archivos).
 - **-g <nuevo_grupo_primario>**: Cambia el grupo primario.
 - **-G <lista_grupos_secundarios>**: Establece los grupos secundarios. **¡Cuidado!** Esto *reemplaza* los grupos secundarios existentes, no añade.
 - **-aG <lista_grupos_secundarios>**: **Añade** el usuario a grupos secundarios sin eliminar los existentes. **Diferencia importante:** -aG es más común en Debian/Ubuntu, -G sin -a es más común en RHEL/Fedora para establecer la lista completa. Aunque **usermod** en ambas ramas suele soportar -aG. Siempre verifica la documentación (**man usermod**).
 - **-L**: Bloquea la contraseña del usuario (lo deshabilita sin eliminar la cuenta).
 - **-U**: Desbloquea la contraseña.
 - **-e <fecha_caducidad>**: Cambia fecha de caducidad.
 - **-f <dias_inactivo>**: Cambia días inactivos.

4. **passwd**: Establece o cambia la contraseña de un usuario.

- **passwd**: Permite al usuario cambiar su propia contraseña.
- **sudo passwd <nombre_usuario>**: Permite a root cambiar la contraseña de cualquier usuario (sin necesidad de conocer la anterior).
- **passwd -l <nombre_usuario>**: Bloquea la contraseña del usuario (similar a **usermod -L**).

- `passwd -u <nombre_usuario>`: Desbloquea la contraseña (similar a `usermod -U`).
 - `passwd -d <nombre_usuario>`: Elimina la contraseña del usuario (permite iniciar sesión sin contraseña - ¡riesgoso!).
5. **chage**: Cambia la información de antigüedad de la contraseña de un usuario (Password Aging).
- `sudo chage [opciones] <nombre_usuario>`
 - `chage -l <nombre_usuario>`: Lista la información actual de antigüedad de la contraseña.
 - `-E <fecha>`: Establece la fecha de caducidad de la cuenta.
 - `-I <días>`: Establece el número de días que la cuenta permanece activa después de que la contraseña caduca.
 - `-M <días>`: Establece el número máximo de días entre cambios de contraseña.
 - `-m <días>`: Establece el número mínimo de días entre cambios de contraseña.
 - `-W <días>`: Establece el número de días de advertencia antes de que caduque la contraseña.
6. **groupadd**: Crea un nuevo grupo.
- `sudo groupadd <nombre_grupo>`
 - `sudo groupadd -g <gid> <nombre_grupo>`: Especifica el GID.
7. **groupdel**: Elimina un grupo.
- `sudo groupdel <nombre_grupo>`: Solo se puede eliminar si ningún usuario lo tiene como grupo primario.
8. **groupmod**: Modifica un grupo existente.
- `sudo groupmod [opciones] <nombre_grupo>`
 - `-n <nuevo_nombre>`: Cambia el nombre del grupo.
 - `-g <nuevo_gid>`: Cambia el GID (riesgoso).

Herramientas para Cambiar de Usuario o Grupo:

1. **su (substitute user o switch user)**:
 - `su [-l] [<usuario>]`: Cambia al usuario especificado.
 - `su`: Si no se especifica usuario, cambia a `root`.
 - `su -`: Realiza un login completo como el usuario destino (lee sus archivos de configuración de shell de inicio de sesión, cambia al directorio home del usuario, etc.). Es la forma recomendada para cambiar a `root`.
 - Requiere la contraseña del usuario destino.
2. **sudo (substitute user do)**:
 - Permite a usuarios autorizados ejecutar comandos como otro usuario (por defecto, `root`), sin conocer la contraseña del usuario destino, sino usando su propia contraseña (o ninguna).
 - La configuración se define en `/etc/sudoers` (editado con `visudo` para evitar errores de sintaxis que puedan bloquear el acceso `sudo`).

- `sudo <comando> [argumentos]`: Ejecuta el comando como root.
- `sudo -u <otro_usuario> <comando> [argumentos]`: Ejecuta el comando como otro usuario.

3. **newgrp**:

- Cambia el GID primario *efectivo* de la shell actual y de los comandos posteriores al grupo especificado. Debes ser miembro de ese grupo.
- `newgrp <nombre_grupo>`: Cambia al grupo especificado.

Plantillas para Nuevos Usuarios (/etc/skel):

El contenido del directorio `/etc/skel/` se copia automáticamente al nuevo directorio personal de un usuario cuando este se crea con la opción `-m` (o si la distribución lo hace por defecto). Contiene archivos de configuración por defecto (`.bashrc`, `.profile`, directorios como `Desktop`, `Documents`). Es útil para proporcionar un entorno inicial coherente para todos los nuevos usuarios.