**USUARIOS/GRUPOS**

CREACIÓN USUARIOS

14.1 Introducción

Este es Lab 14: 14.7 Crear un Usuario Mediante la realización de esta práctica de laboratorio, los estudiantes aprenderán acerca de cómo crear una nueva cuenta de usuario, establecer la contraseña inicial para esta cuenta, y realizar otras modificaciones, como por ejemplo hacerlos miembros de un grupo secundario.

En este laboratorio llevarás a cabo las siguientes tareas:

* Crear un nuevo usuario con el comando useradd
* Establecer y reiniciar la contraseña de un usuario con el comando passwd
* Realizar cambios en la cuenta de usuario con el comando usermod

## 14.2 Crear Usuarios y Grupos

En esta tarea vas a crear cuentas de usuario y de grupo.

Las cuentas de grupo pueden ser de utilidad para poder asignar permisos de archivos compartidos por un grupo de usuarios.

Las cuentas de usuario en las distribuciones de Linux basadas en Red Hat, al igual que la distribución CentOS, comienzan con el primer ID de usuario (UID) hasta 500, el siguiente UID de 501, y así sucesivamente. La tendencia actual seguida de muchas otras distribuciones es tener el primer UID de 1000, el segundo de 1001, y así sucesivamente.

Si gestionas cuentas para múltiples sistemas, entonces es bueno disponer de un servidor de autenticación basado en la red, donde las cuentas se pueden crear una vez y utilizar en muchas máquinas. De lo contrario, la gestión de varias cuentas en varias máquinas puede ser un reto, ya que puede ser difícil de asegurar que el usuario, y todos los grupos a los que pertenecen tienen los mismos UID y GID en todas las máquinas.

Otro problema con las cuentas en muchas máquinas es que puede ser difícil mantener las contraseñas para cada cuenta sincronizada en todas las máquinas.

Administrar las cuentas de usuarios locales sigue siendo útil para máquinas individuales, incluso si no tienen acceso a un servidor de autenticación basado en la red. En esta práctica de laboratorio vas a administrar cuentas de usuario y de grupo locales.

14.2.1 Paso 1

Con el fin de administrar las cuentas de usuario y de grupo, tendrás que cambiar tu usuario al root con el siguiente comando:

su - (Proporciona la contraseña "netlab123" cuando veas el prompt)

## 14.2.2 Paso 2

Utiliza el comando groupadd para crear un grupo llamado «research» (significa «investigación» en español):

groupadd -r research

**root@localhost:~#** groupadd -r research **root@localhost:~#**

El grupo research que se acaba de agregar se añadió al rango reservado (del 1 al 999), porque utilizamos la opción -r. Los identificadores de grupo (GID) se asignan automáticamente con un valor inferior al UID de usuario normal más bajo con esta opción. El comando groupadd modifica el archivo /etc/group en el que se almacena la información acerca de la cuenta del grupo.

El comando groupmod se podría utilizar con una opción -n para cambiar el nombre de este grupo o la opción -g para cambiar el GID para este grupo. El comando groupdel se puede utilizar para eliminar este grupo, siempre y cuando no haya sido creado como grupo principal para un usuario.

## 14.2.3 Paso 3

Utiliza el comando getent para recuperar la información acerca del nuevo grupo:

getent group research

La salida debería ser similar a la siguiente, aunque el GID que le fue asignado puede ser diferente:

Ahora que se creó el grupo research, usuarios existentes o nuevos pueden ser miembros de este grupo. La opción -G de usermod debe tener una lista separada por comas de todos los grupos secundarios a los que pertenece el usuario.

Cuando se utiliza usermod con la opción -a y -G, entonces sólo hay que especificar al grupo nuevo y añadirlo como miembro de los grupos secundarios existentes.

14.2.4 Paso 4

Utiliza el comando usermod para agregar el grupo research como un grupo secundario para el usuario sysadmin:

usermod -aG research sysadmin

**root@localhost:~#** usermod -aG research sysadmin **root@localhost:~#**

Los usuarios que han iniciado sesión de forma activa en el sistema no podrán pertenecer a los grupos nuevos hasta que inicien la sesión en el sistema la próxima vez.

## 14.2.5 Paso 5

Hay varios comandos para verificar la nueva pertenencia al grupo. Utiliza los comandos groups, id y getent para verificar si el sysadmin pertenece al grupo:

groups sysadmin id sysadmin getent group research

La salida de los comandos anteriores debería ser similar a la siguiente:

**root@localhost:~#** groups sysadmin sysadmin : sysadmin adm sudo research **root@localhost:~#** id sysadmin uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),4(adm),27(sudo),999(research) **root@localhost:~#** getent group research research:x:999:sysadmin **root@localhost:~#**

El comando useradd creará una nueva cuenta de usuario y, en las distribuciones basadas en Red Hat, un nuevo grupo de ese usuario. Este nuevo grupo llevará el nombre de usuario y ese será su grupo primario.

Las distribuciones Red Hat basadas en el uso de lo que se conoce como «Grupos privados de usuario», o UPG, cada usuario es un miembro principal de su propio grupo privado.

Para las distribuciones que no utilizan un UPG, todos los nuevos usuarios pertenecen al grupo users como su grupo primario.

14.2.6 Paso 6

Crea un nuevo usuario llamado student siendo éste el miembro secundario del grupo research y miembro principal de su propio grupo privado. Utiliza un comentario de Linux Student que aparecerá como nombre completo del usuario cuando lo realizan al iniciar la sesión en un entorno gráfico. Asegúrate de que su directorio home se creará especificando la opción -m:

useradd -G research -c 'Linux Student' -m student

**root@localhost:~#** useradd -G research -c 'Linux Student' -m student **root@localhost:~#**

La información de usuario se almacena en los archivos /etc/passwd y /etc/shadow. La información de grupo usuario se puede encontrar en los archivos /etc/passwd y /etc/group.

## 14.2.7 Paso 7

Utilizando el comando getent, vuelve a visualizar los miembros del grupo research, pero también utiliza getent para mostrar el grupo student , y las bases de datos passwd y shadow para el usuario student:

getent group research getent group student getent passwd student getent shadow student

Ahora la salida debe mostrar que tanto sysadmin como student son miembros secundarios del grupo research.

El GID del grupo student coincide con el cuarto campo de la información passwd. Como resultado, student es el miembro principal del grupo student.

Finalmente, el signo ! que aparece en el campo de la contraseña (segundo campo) del archivo shadow, muestra que la contraseña para student no fue configurada.

## 14.2.8 Paso 8

Utiliza el comando passwd para establecer la contraseña, netlab123 para el usuario student y vuelve a visualizar le entrada del archivo shadow para el usuario student:

passwd student (escriba la misma contraseña dos veces) getent shadow student

La salida del archivo /etc/shadow, ahora muestra una contraseña cifrada en el segundo campo:

## 14.2.9 Paso 9

El hecho de que un usuario tiene una contraseña, no significa que alguna vez haya iniciado sesión en el sistema. Utiliza el comando last para ver si el usuario student inició la sesión en alguna ocasión:

last last student

La salida del comando last debería mostrar que el usuario sysadmin había iniciado la sesión antes, pero no el usuario student:

También hay una lastb comando, que funciona de forma similar al comando last salvo que muestra los intentos de inicio de sesión «malos» o fallidos.

Si ya no quieres que el usuario student tenga acceso al sistema, utiliza el comando usermod -L student para «bloquear» la cuenta. La cuenta se puede desbloquear con el comando usermod -U student.

Una solución más permanente para impedir el acceso a la cuenta student sería eliminar la cuenta, ya sea con el comando userdel student, o bien con userdel -r student. Utilizando la opción -r con el comando userdel elimina el directorio personal del usuario y el correo, además de eliminar la cuenta del usuario.

## 14.2.10 Paso 10

Borra la cuenta student y elimina el directorio home del usuario:

userdel -r student

La ejecución del comando debería tener este aspecto: