



Administración de Linux

Usuarios, grupos y permisos

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Contenidos

- Administración de usuarios
 - Creación, modificación, eliminación
- Atributos de las contraseñas
- Administración de permisos en archivos y directorios
- Cuota de disco

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Admin. de usuarios y grupos

- Las políticas de usuarios y grupos definen:
 - Niveles de acceso al sistema de archivos
 - Forzar o no cambios periódicos en las password
 - Imponer o no límites en el uso de la CPU y memoria
 - Habilitar o no cuotas en disco

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Archivo /etc/passwd

- Es la base de datos estándar de usuarios
- Cada entrada en este archivo representa un usuario del sistema
- Su contenido es requerido en el momento de hacer "login" al sistema y también por otros programas

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Archivo /etc/passwd

```
root@server:/  
Archivo Editar Ver Terminal Ir a Ayuda  
rpm:x:37:37:/:var/lib/rpm:/sbin/nologin  
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin  
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin  
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin  
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin  
mailnull:x:47:47:/:var/spool/mqueue:/sbin/nologin  
smmsp:x:51:51:/:var/spool/mqueue:/sbin/nologin  
pcap:x:77:77:/:var/arpwatch:/sbin/nologin  
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin  
ntp:x:38:38:/:etc/ntp:/sbin/nologin  
gdm:x:42:42:/:var/gdm:/sbin/nologin  
desktop:x:80:80:desktop:/var/lib/menu/kde:/sbin/nologin  
apache:x:48:48:Apache:/var/www:/sbin/nologin  
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin  
squid:x:23:23:/:var/spool/squid:/sbin/nologin  
named:x:25:25:Named:/var/named:/sbin/nologin  
cguerci:x:500:0:/:home/cguerci:/bin/bash  
spabon:x:501:501:/:home/spabon:/bin/bash  
redhat:x:503:503:/:home/redhat:/bin/bash  
soporte:x:504:504:/:home/soporte:/bin/bash  
tecnico:x:505:508:/:home/tecnico:/bin/bash  
contable:x:506:509:/:home/contable:/bin/bash  
legislacion:x:507:510:/:home/legislacion:/bin/bash  
[root@Server ~]#
```

Ing. Raúl Eduardo Tschmaz
AUS Gustavo Ceresoli



Archivo /etc/passwd

- Cada línea del archivo /etc/passwd está compuesta de campos separados por " : "
 - Nombre de usuario
 - Contraseña
 - ID de usuario
 - ID de grupo
 - Comentarios
 - Directorio home
 - Shell

Ing. Raúl Eduardo Tschmaz
AUS Gustavo Ceresoli



Creación de cuentas

- Los usuarios pueden crearse con el comando `useradd`
 - Se asigna un valor UID y GID por defecto
 - El nombre del grupo es igual al nombre de usuario
 - Los UID y GID son iguales y por encima de 500

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Creación de cuentas

- La información de los grupos de usuarios están en `/etc/group`
- Sintaxis de `useradd`
 - `useradd (parámetros) (nombre)`

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Comando useradd

- -c: comentario
- -d: directorio home
- -e: fecha de expiración
- -g: grupo
- -G: grupos
- -s: shell
- -p: password

```
root@server:~  
Archivo Editar Ver Terminal Ir a Ayuda  
[root@server root]# useradd -c 'usuario de prueba' -e 2004-12-24 ipghost  
[root@server root]# cat /etc/passwd | grep ipghost  
ipghost:x:505:505:usuario de prueba:/home/ipghost:/bin/bash  
[root@server root]#
```

Ing. Diego Ivan Tschmaz
Ing. Carlos Tuñateoli



Modificación de cuentas

- La modificación de los datos de las cuentas de usuario se realiza con el comando usermod
- Las opciones son similares a useradd

```
root@server:~  
Archivo Editar Ver Terminal Ir a Ayuda  
[root@server /]# usermod -d /cursos/curso2 -g miscelaneas ipghost  
[root@server /]# cat /etc/passwd | grep ipghost  
ipghost:x:505:507:usuario de prueba:/cursos/curso2:/bin/bash
```

Ing. Raúl Eduardo Tschmaz
AUS Gustavo Ceresoli



Eliminación de cuentas

- Se utiliza el comando `userdel`
- Los datos del usuario no son eliminados
- Con la opción `-r` se elimina su directorio `home`

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Administración de password

- El comando `chage` permite establecer la política de tiempos de cambios de contraseñas
 - Las contraseñas configuradas a un usuario no expiran nunca
 - Se establece un tiempo de vida máximo y mínimo para las contraseñas

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Administración de password

§ Sintaxis del comando

– chage (parámetros) (usuario)

§ Parámetros

- | | |
|-----------------------------------|-----------------------------------|
| – m: Cant. mínima de días | – E: Fecha de expiración |
| – M: Cant. máxima de días | – W: Cant. de días de advertencia |
| – I: Cant. de días de inactividad | – l: muestra los valores |

Ing. Diego Ivan Tschnaz
Ing. Carlos Iván Ceresoli



Creación y mod. de grupos

- El archivo /etc/group define los grupos

```
contable:x:509:  
empleados:x:511:soporte,sueldos,compras  
directivos:x:512:rrhh,comercial,tecnica  
planeamiento:x:513:  
logistica:x:514:  
rrhh:x:515:  
comercial:x:516:  
tecnica:x:517:  
sueldos:x:518:  
compras:x:519:  
[root@Server ~]#
```

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Creación y mod. de grupos

- Cada línea del archivo representa un grupo y está compuesta por campos separados por ":"
 - nombre del grupo
 - la password del grupo
 - el GID
 - lista de nombres de usuarios separada por comas que pertenecen al grupo

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Creación y mod. de grupos

- Comandos para la administración de grupos:
 - groupadd nombre
 - groupmod nombre
 - groupdel nombre

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Manipulación de propietarios

- Cada uno de los archivos y directorios creados en Linux pertenecen a un dueño y a un grupo
 - En un principio es el usuario que lo crea con el grupo primario al cual pertenece el usuario
 - Se puede visualizar mediante el comando `ls -l`

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



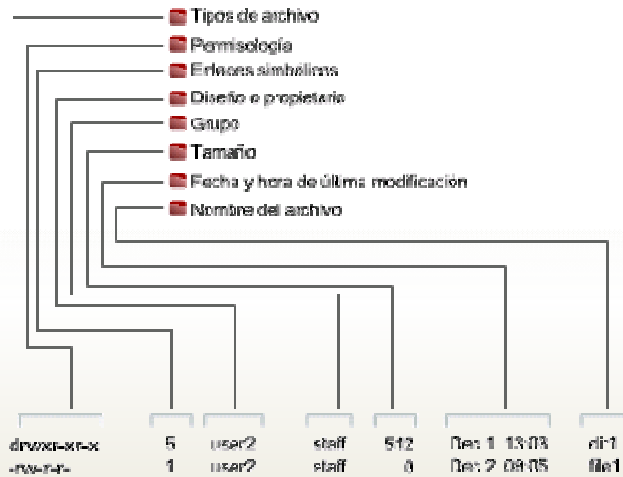
Manipulación de propietarios

- Para modificar al propietario o grupo de un archivo se usan los comandos
 - `chown (usuario) (archivo)`
 - `chgrp (grupo) (archivo)`
 - `chown (usuario).(grupo) (archivo)`

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Permisos de archivos



Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Permisos de archivos

- Hay definidos tres **niveles de acceso** , denominados:
 - Usuario (u)
 - Grupo (g)
 - Otros (o)

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Permisos de archivos

- Por cada nivel de acceso hay definidos tres **modos de acceso**:
 - Lectura (r)
 - Escritura (w)
 - Ejecución (x)

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Permisos de archivos

- El conjunto de niveles y modos de acceso queda definido por 9 caracteres

– $\underbrace{rwx}_{U} \underbrace{rwx}_{G} \underbrace{rwx}_{O}$

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Permisos de archivos

Permisos	Símbolo	Archivo	Directorio
Lectura	r	El archivo se puede ver o copiar	El contenido puede ser listado con el comando ls. (Para ver el listado largo se necesita permisos de ejecución)
Escritura	w	El contenido se puede modificar	Se pueden agregar o eliminar archivos (se necesita también permisos de ejecución)
Ejecución	x	Se puede ejecutar	Permite buscar archivos dentro del directorio
Sin permiso	-	Permiso denegado	Permiso denegado

Ing. Raúl Eduardo Tschmaz
AUS Gustavo Ceresoli



Permisos de archivos

```
$ls -l .profile
-rw-r--r-- 1 user2 staff 582 Mar 16 15:07 .profile
```

Type	User	Group	Other
-	rw-	r--	r--

```
$ls -l /bin/mkdir
-r-xr-xr-x 1 root bin 13168 Jan 5 2000 /bin/mkdir
```

Type	User	Group	Other
-	r-x	r-x	r-x

Ing. Raúl Eduardo Tschmaz
AUS Gustavo Ceresoli



Cambio de permisos

- Los permisos de archivos y directorios pueden cambiarse utilizando el comando `chmod` (cambiar modo [change mode])
 - Generalmente no es necesario realizar cambio de permisos en los archivos
 - Los scripts son un ejemplo de archivos que necesitan cambios en sus permisos

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Modos de establecer permisos

- El comando `chmod` es utilizado por el propietario de un archivo (o superusuario) para cambiar los permisos de un archivo
- Los dos modos de operación con el comando `chmod` son
 - simbólico [symbolic] (o relativo)
 - octal (o absoluto)

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Modo simbólico o relativo

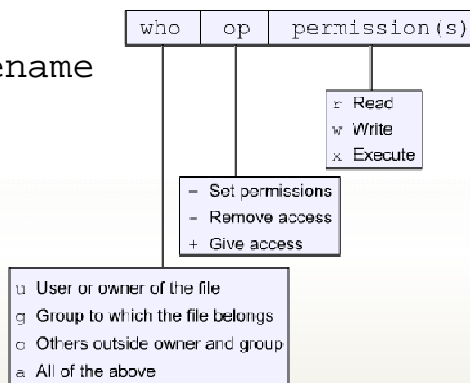
- **Modo Simbólico**
 - Utiliza combinaciones de letras y símbolos para agregar o quitar permisos a diversas categorías de usuarios
 - También se denomina modo relativo
- **Modo Octal**
 - Utiliza números octales para representar permisos de archivos
 - También se denomina modo absoluto o numérico

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Modo simbólico

- **Formato del comando:**
`$chmod mode filename`
- **Donde mode es:**



Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Ejemplo de modo simbólico

```
Remove (deny) group read permission
$ ls -l dante
-rw-r--r-- 1 user2 staff2 Jun 11 1:44 dante
$ chmod g-r dante
$ ls -l dante
-rw----r-- 1 user2 staff2 Jun 11 1:44 dante

Deny read permission to others
$ chmod o-r dante
$ ls -l dante
-rw----- 1 user2 staff2 Jun 11 1:44 dante

Add execute permission for owner, and read permission for group and others
$ chmod u+x,go+r dante
$ ls -l dante
-rwxr--r-- 1 user2 staff2 Jun 11 1:44 dante
Note: There is no space after u+x and before go+r, although there is a
comma between them.

Set permissions to read and write for everyone
$ chmod a=rw dante
$ ls -l dante
-rw-rw-rw- 1 user2 staff2 Jun 11 1:44 dante
```

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Modo octal o absoluto

- Este modo también se denomina absoluto ya que los permisos que usted aplique reemplazan a los ya existentes
- Existen tres permisos posibles para cada conjunto (propietario, grupo y otros): r, w y x
 - A cada conjunto de permisos se puede asignarse un valor numérico (de 0 a 7) dependiendo de qué permisos se aprueban
 - El modo se denomina octal ya que existen ocho valores posibles para cada conjunto de permisos

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Valores octales

Octal Value	Permissions
4	Read
2	Write
1	Execute

Octal Value	Sum of Permission Category Values	Corresponding Permissions	Definition
7	4 + 2 + 1	r w x	Read, Write and Execute
6	4 + 2 + 0	r w -	Read and Write
5	4 + 0 + 1	r - x	Read and Execute
4	4 + 0 + 0	r - -	Read only
3	0 + 2 + 1	- w x	Write and Execute
2	0 + 2 + 0	- w -	Write only
1	0 + 0 + 1	- - x	Execute only
0	0 + 0 + 0	- - -	No permissions

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Valores octales

Octal Value	Permissions	Notes
555	r-xr-xr-x	Standard permissions for executable UNIX commands such as cat and pwd
644	rW-r--r--	Default permissions for File
755	rwxr-xr-x	Default permissions for directories
744	rwxr--r--	Typical Permissions for user script file
777	rwxrwxrwx	All permissions to everyone (open)

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Ejemplos

Give User, Group and Others Read and Execute permissions

```
$ ls -l dante  
-rw-rw-rw- 1 user2 staff2 Jun 11 11:54 dante
```

```
$ chmod 555 dante
```

```
$ ls -l dante  
-r-xr-xr-x 1 user2 staff2 Jun 11 11:54 dante
```

Change User and Group permissions to include Write access

```
$ chmod 775 dante
```

```
$ ls -l dante  
-rwxrwxr-x 1 user2 staff2 Jun 11 11:54 dante
```

Change Group permission to Read and Execute

```
$ chmod 755 dante
```

```
$ ls -l dante  
-rwxr-xr-x 1 user2 staff2 Jun 11 11:54 dante
```

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Bits especiales

- Además de los simples permisos de lectura, escritura y ejecución existen otros tipos de permisos que se pueden aplicar a los archivos y directorios, llamados:
 - bits SUID
 - bits SGID
 - bit Sticky

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Bits especiales

SUID/SGI

- Permiten a los usuarios acceder a un archivo ejecutable con los permisos del dueño del mismo (SUID) o su grupo (SGID)
- Permiten correr programas sólo ejecutables como root.
- Muestran una "s" en el campo de ejecución del dueño (SUID) o grupo (SGID) del archivo
- SUID puede configurarse con el comando `chmod` y el valor octal `4000`
- SGID puede configurarse con el comando `chmod` y el valor octal `2000`

Bit Sticky

- Protege a los archivos de un directorio subdirectorio
- Para un directorio con el bit sticky configurado, un archivo sólo puede ser eliminado por su dueño o root
- Aparece como una letra "t" en el campo de ejecución de "otros"
- Sólo el dueño del directorio y root pueden configurar el bit sticky, con el comando `chmod` y el valor octal `1000`

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Bits especiales

- Ejemplos
 - `chmod o+t /home/share`
 - `chmod u+s ejecutable-01`
 - `chmod g+s ejecutable-02`
 - `chmod g+s /home/grupo-teleinformática`

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Preguntas



Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Quotas

- Permiten limitar la cantidad de recursos de disco a los que los usuarios pueden acceder
- Con esto se puede evitar que un usuario ocupe demasiado espacio en disco, o bien una partición se llene

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Quotas

- Permiten controlar
 - Cantidad de espacio ocupado (bloques)
 - Cantidad de archivos creados (i-nodos)
- Se aplican a cada partición de manera independiente
- Es necesario indicarle a “mount” que el dispositivo a montar usará quotas

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Implementación de Quotas

- La implementación de cuotas requiere de los siguientes pasos:
 - Habilitación de cuotas por sistema de archivo, modificando el archivo /etc/fstab.
 - Re-montar los sistemas de archivos.
 - Crear los archivos de cuota y generar la tabla de uso de disco.
 - Asignar cuotas
 - Activación y desactivación de cuotas.

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Implementación de Quotas

- **Habilitación de cuotas:**
 - Se debe editar el archivo `/etc/fstab` agregando las opciones `usrquota` y/o `grpquota` sobre aquellos sistemas de archivos que requieran cuotas

```
/dev/hdb1    /home    ext3    defaults,usrquota,grpquota    1 2
```

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Implementación de Quotas

- **Re-montaje:** Modificado el `fstab` se puede remontar el dispositivo para habilitar las opciones:
- `mount -o remount (dispositivo)`

```
[root@server:~]mount -o remount /dev/hda1
```

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Implementación de Quotas

- Creación de los archivos cuota: una vez remontado, el sistema está capacitado para trabajar con cuotas.
 - Se deben crear los archivos que contengan los registros de uso del dispositivo
 - El comando quotacheck genera los archivo de cuotas aquota.user y aquota.group

```
[root@server:~]quotachek -c /dev/hdb1
```

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Implementación de Quotas

- Asignación de cuotas: el superusuario (root) puede configurar cuotas individualmente para cada usuario distinto, utilizando el comando edquota (nombre de usuario)
 - Este comando invoca un editor de texto
 - Se deben establecerse un límite inicial (soft) y un límite final (hard)

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Implementación de cuotas

- Monitoreo de cuotas
 - Comando quota: lo utiliza un usuario para conocer su estado de uso, tiempo de gracia y disponibilidad
 - Comando repquota: lo utiliza el administrador para obtener un listado del uso de un dispositivo clasificado por usuario

Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli



Preguntas



Ing. Raúl Eduardo Tschnaz
AUS Gustavo Ceresoli