Gestión de usuarios y grupos locales- Redes PYMES

Índice general de la serie: Redes de Computadoras para las PYMES: Introducción

Autor: Federico Antonio Valdes Toujague
federicotoujague@gmail.com
http://blog.desdelinux.net/author/fico

¡Hola amigas y amigos!

Este artículo es continuación de Squid + Autenticación PAM en CentOS 7- Redes PYMES.

Los sistemas operativos UNIX/Linux ofrecen un ambiente multiusuario REAL, en los cuales muchos usuarios pueden trabajar simultáneamente sobre el mismo sistema y compartir recursos tales como procesadores, discos duros, memoria, interfaces de redes, dispositivos insertados en el sistema, etcétera.

Por ello, los Administradores de Sistemas están obligados a gestionar de forma continua a los usuarios y grupos del sistema y a formular e implementar una buena estrategia de administración.

A continuación veremos de forma muy concisa los aspectos generales de ésta importante actividad en la Administración de Sistemas Linux.

A veces es mejor ofrecer Utilidad y luego Necesidad.

Éste es un típico ejemplo de ese orden. Primero mostramos como implementar un servicio de Internet Proxy con Squid y usuarios locales. Ahora nos debemos preguntar:

- *¿cómo puedo implementar servicios de redes en una LAN UNIX/Linux a partir de usuarios locales y con una **seguridad aceptable***?.

No importa que, además, estén conectados a ésta red clientes Windows. Solo importa la necesidad de cuáles servicios necesita la Red PYME y cuál es la forma mas sencilla y barata de implementarlos.

- ***¿**Acaso el mecanismo de autenticación en el nacimiento de la **ARPANET**, **Internet** y demás redes **W**ide **A**rea **N**etwork o **L**ocal **A**rea **N**etwork iniciales se basó en **LDAP**, **Directory Service**, o en **Microsoft LSASS**, o en **Active Directory**, o mediante **Kerberos**?, por solo mencionar algunos*.

Una buena pregunta que cada cual debe buscar sus respuestas. Invito a que realicen una búsqueda por el término "*authentication*" en la Wikipedia en inglés, que por mucho es la mas completa y coherente en lo que a contenido original -en inglés- se refiere.

Acorde a la Historia y a *grosso modo*, primero fue la **Autenticación** y **Autorización** **locales**, después **NIS** *Network Information System* desarrollado por la Sun Microsystem y conocido también como **Yellow Pages** o ***yp***, y después **LDAP** *Lightweight Directory*

Access Protocol.

Lo de "***Seguridad Aceptable***" viene a colación debido a que muchas veces nos preocupamos por la seguridad de nuestra red local, mientras accedemos a Facebook, Gmail, Yahoo, etcétera -por mencionar solos unos pocos- y entregamos a Nuestra Privacidad en ellos. Y miren Ustedes la gran cantidad de artículos y documentales que al respecto de la *No Privacidad en Internet* existen.

Nota sobre CentOS y Debian

CentOS/Red Hat y Debian tienen su propia filosofía en cuanto a cómo implementar la seguridad, que no difiere en aspectos fundamentales. No obstante afirmamos que las dos son muy estables, seguras y fiables. Por ejemplo, en CentOS el contexto SELinux viene habilitado por defecto. En Debian debemos instalar el paquete ***selinux-basics***, lo que indica que también podemos utilizar SELinux.

En CentOS, FreeBSD, y otros sistemas operativos, se crea el grupo -del sistema- ***wheel*** para permitir el acceso como *root* solamente a los usuarios del sistema que pertenezcan a ese grupo. Lea */usr/share/doc/pam-1.1.8/html/Linux-PAM_SAG.html*, y */usr/share/doc/pam-1.1.8/html/Linux-PAM_SAG.html*. Debian no incorpora un grupo *wheel*.

Archivos y comandos principales

Archivos

Los principales archivos relacionados con la gestión de los usuarios locales en un sistema operativo Linux son:

CentOS y Debian

- ***/etc/passwd***: información de las cuentas de usuario.
- ***/etc/shadow***: información de seguridad de las cuentas de usuario.
- ***/etc/group***: información de las cuentas de grupos.
- ***/etc/gshadow***: información de seguridad de las cuentas de grupo.
- ***/etc/default/useradd***: valores por defecto para la creación de las cuentas.
- ***/etc/skel/***: directorio que contiene los archivos por defecto que se incluiran en el directorio HOME del nuevo usuario.
- ***/etc/login.defs***: suite de configuración de la seguridad de las contraseñas.

Debian

- ***/etc/adduser.conf***: valores por defecto para la creación de las cuentas.

Comandos en CentOS y Debian

```
[root@linuxbox ~]# chpasswd -h  # Actualiza contraseñas en modo batch
Modo de uso: chpasswd [opciones]

Opciones:
  -c, --crypt-method METHOD     the crypt method (one of NONE DES MD5 SHA256 SHA512)
  -e, --encrypted               se cifran las contraseñas proporcionadas
  -h, --help                    muestra este mensaje de ayuda y termina
  -m, --md5                     cifra la contraseña en claro utilizando
                                el algoritmo MD5
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --sha-rounds              número de rondas SHA para los algoritmos
                                de cifrado SHA*

# batch: ejecuta comandos cuando la carga del sistema lo permite. En otras palabras
# cuando la carga promedio cae por debajo de 0.8 o el valor especificado al invocar
# el comando atd. Mas información man batch.

[root@linuxbox ~]# gpasswd -h   # Declara Administradores en /etc/group y /etc/gshadow
Modo de uso: gpasswd [opciones] GRUPO

Opciones:
  -a, --add USUARIO             añade USUARIO al GRUPO
```

```
  -d, --delete USUARIO          elimina USUARIO del GRUPO
  -h, --help                    muestra este mensaje de ayuda y termina
  -Q, --root CHROOT_DIR         directory to chroot into
  -r, --delete-password         remove the GROUP's password
  -R, --restrict                restringe el acceso a GRUPO a sus miembros
  -M, --members USUARIO,...     establece la lista de miembros de GRUPO
  -A, --administrators ADMIN,...
                                establece la lista de administradores de GRUPO
Excepto las opciones -A y -M, las opciones no se pueden combinar.

[root@linuxbox ~]# groupadd -h  # Crea un nunevo grupo
Modo de uso: groupadd [opciones] GRUPO

Opciones:
  -f, --force                   termina si el grupo ya existe, y cancela -g
                                si el GID ya se está en uso
  -g, --gid GID                 utiliza GID para el nuevo grupo
  -h, --help                    muestra este mensaje de ayuda y termina
  -K, --key CLAVE=VALOR         sobrescribe los valores predeterminados de
                                «/etc/login.defs»
  -o, --non-unique              permite crear grupos con GID (no únicos)
                                duplicados
  -p, --password CONTRASEÑA     utiliza esta contraseña cifrada para el nuevo
                                grupo
  -r, --system                  crea una cuenta del sistema
  -R, --root CHROOT_DIR         directory to chroot into

[root@linuxbox ~]# groupdel -h  # Borra un grupo existente
Modo de uso: groupdel [opciones] GRUPO

Opciones:
  -h, --help                    muestra este mensaje de ayuda y termina
  -R, --root CHROOT_DIR         directory to chroot into

[root@linuxbox ~]# groupmems -h # Declara Administradores en el grupo primario de un usuario
Modo de uso: groupmems [opciones] [acción]

Opciones:
  -g, --group GRUPO             cambia el nombre del grupo en lugar del grupo
                                del usuario (sólo lo puede hacer el
                                administrador)
  -R, --root CHROOT_DIR         directory to chroot into

Acciones:
  -a, --add USUARIO             añade USUARIO a los miembros del grupo
  -d, --delete USUARIO          elimina USUARIO de la lista de miembros del
                                grupo
  -h, --help                    muestra este mensaje de ayuda y termina
  -p, --purge                   purga todos los miembros del grupo
  -l, --list                    lista los miembros del grupo

[root@linuxbox ~]# groupmod -h  # Modifica la definición de un grupo
Modo de uso: groupmod [opciones] GRUPO

Opciones:
  -g, --gid GID                 cambia el identificador del grupo a GID
  -h, --help                    muestra este mensaje de ayuda y termina
  -n, --new-name GRUPO_NUEVO    cambia el nombre a GRUPO_NUEVO
  -o, --non-unique              permite utilizar un GID duplicado (no único)
  -p, --password CONTRASEÑA     cambia la contraseña a CONTRASEÑA (cifrada)
  -R, --root CHROOT_DIR         directory to chroot into

[root@linuxbox ~]# grpck -h     # Verifica la integridad de un archivo de grupos
Modo de uso: grpck [opciones] [grupo [gshadow]]
```

```
Opciones:
  -h, --help                    muestra este mensaje de ayuda y termina
  -r, --read-only               display errors and warnings
                                but do not change files
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --sort                    sort entries by UID

[root@linuxbox ~]# grpconv
# Comandos asociados: pwconv, pwunconv, grpconv, grpunconv
# Se utiliza para convertir desde y hacia contraseñas shadow y grupos
# Los cuatro comandos operan sobre los archivos /etc/passwd, /etc/group, /etc/shadow,
# y /etc/gshadow. Para mas información man grpconv.

[root@linuxbox ~]# sg -h        # Ejecuta un comando con un diferente group ID o GID
Modo de uso: sg grupo [[-c] orden]

[root@linuxbox ~]# newgrp -h    # Cambia el GID actual durante un inicio de sesión
Modo de uso: newgrp [-] [grupo]

[root@linuxbox ~]# newusers -h  # Actualiza y crea nuevos usuarios en modo batch
Modo de uso: newusers [opciones]

Opciones:
  -c, --crypt-method METHOD     the crypt method (one of NONE DES MD5 SHA256 SHA512)
  -h, --help                    muestra este mensaje de ayuda y termina
  -r, --system                  crea cuentas del sistema
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --sha-rounds              número de rondas SHA para los algoritmos
                                de cifrado SHA*

[root@linuxbox ~]# pwck -h      # Verifica la integridad de los archivos de contraseñas
Modo de uso: pwck [opciones] [passwd [shadow]]

Opciones:
  -h, --help                    muestra este mensaje de ayuda y termina
  -q, --quiet                   report errors only
  -r, --read-only               display errors and warnings
                                but do not change files
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --sort                    sort entries by UID

[root@linuxbox ~]# useradd -h   # Crea un nuevo usuario o actualiza la información por
                                # defecto del nuevo usuario
Modo de uso: useradd [opciones] USUARIO
             useradd -D
             useradd -D [opciones]

Opciones:
  -b, --base-dir DIR_BASE       directorio base para el directorio personal
                                de la nueva cuenta
  -c, --comment COMENTARIO      campo GECOS de la nueva cuenta
  -d, --home-dir DIR_PERSONAL   directorio personal de la nueva cuenta
  -D, --defaults                imprime o cambia la configuración
                                predeterminada de useradd
  -e, --expiredate FECHA_CADUCIDAD  fecha de caducidad de la nueva cuenta
  -f, --inactive INACTIVO       periodo de inactividad de la contraseña
                                de la nueva cuenta
delgroup
  -g, --gid GRUPO               nombre o identificador del grupo primario de
                                la nueva cuenta
  -G, --groups GRUPOS           lista de grupos suplementarios de la nueva
                                cuenta
  -h, --help                    muestra este mensaje de ayuda y termina
  -k, --skel DIR_SKEL           utiliza este directorio «skeleton» alternativo
  -K, --key CLAVE=VALOR         sobrescribe los valores predeterminados de
```

```
                                «/etc/login.defs»
  -l, --no-log-init             no añade el usuario a las bases de datos de
                                lastlog y faillog
  -m, --create-home             crea el directorio personal del usuario
  -M, --no-create-home          no crea el directorio personal del usuario
  -N, --no-user-group           no crea un grupo con el mismo nombre que el
                                usuario
  -o, --non-unique              permite crear usuarios con identificadores
                                (UID) duplicados (no únicos)
  -p, --password CONTRASEÑA     contraseña cifrada de la nueva cuenta
  -r, --system                  crea una cuenta del sistema
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell CONSOLA           consola de acceso de la nueva cuenta
  -u, --uid UID                 identificador del usuario de la nueva cuenta
  -U, --user-group              crea un grupo con el mismo nombre que el
                                usuario
  -Z, --selinux-user USUARIO_SE  utiliza el usuario indicado para el usuario
                                 de SELinux

[root@linuxbox ~]# userdel -h   # Borra la cuenta de un usuario y archivos relacionados
Modo de uso: userdel [opciones] USUARIO

Opciones:
  -f, --force                   force some actions that would fail otherwise
                                e.g. removal of user still logged in
                                or files, even if not owned by the user
  -h, --help                    muestra este mensaje de ayuda y termina
  -r, --remove                  elimina el directorio personal y el buzón de
                                correo
  -R, --root CHROOT_DIR         directory to chroot into
  -Z, --selinux-user            remove any SELinux user mapping for the user

[root@linuxbox ~]# usermod -h   # Modifica una cuenta de usuario
Modo de uso: usermod [opciones] USUARIO

Opciones:
  -c, --comment COMENTARIO      nuevo valor del campo GECOS
  -d, --home DIR_PERSONAL       nuevo directorio personal del nuevo usuario
  -e, --expiredate FECHA_EXPIR  establece la fecha de caducidad de la
                                cuenta a FECHA_EXPIR
  -f, --inactive INACTIVO       establece el tiempo de inactividad después
                                de que caduque la cuenta a INACTIVO
  -g, --gid GRUPO               fuerza el uso de GRUPO para la nueva cuenta
                                de usuario
  -G, --groups GRUPOS           lista de grupos suplementarios
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                him/her from other groups
  -h, --help                    muestra este mensaje de ayuda y termina
  -l, --login NOMBRE            nuevo nombre para el usuario
  -L, --lock                    bloquea la cuenta de usuario
  -m, --move-home               mueve los contenidos del directorio
                                personal al directorio nuevo (usar sólo
                                junto con -d)
  -o, --non-unique              permite usar UID duplicados (no únicos)
  -p, --password CONTRASEÑA     usar la contraseña cifrada para la nueva cuenta
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell CONSOLA           nueva consola de acceso para la cuenta del
                                usuario
  -u, --uid UID                 fuerza el uso del UID para la nueva cuenta
                                de usuario
  -U, --unlock                  desbloquea la cuenta de usuario
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
```

Comandos en Debian

Debian establece la diferencia entre ***useradd*** y ***adduser***. Recomienda que los Administradores de Sistemas utilicen ***adduser***.

```
root@sysadmin:/home/xeon# adduser -h    # Añade un usuario al sistema
root@sysadmin:/home/xeon# addgroup -h   # Añade un grupo al sistema
adduser [--home DIRECTORIO] [--shell SHELL] [--no-create-home] [--uid ID]
[--firstuid ID] [--lastuid ID] [--gecos GECOS] [--ingroup GRUPO | --gid ID]
[--disabled-password] [--disabled-login] USUARIO
   Añade un usuario normal

adduser --system [--home DIRECTORIO] [--shell SHELL] [--no-create-home] [--uid ID]
[--gecos GECOS] [--group | --ingroup GRUPO | --gid ID] [--disabled-password]
[--disabled-login] USUARIO
   Añade un usuario del sistema

adduser --group [--gid ID] GRUPO
addgroup [--gid ID] GRUPO
   Añade un grupo de usuarios

addgroup --system [--gid ID] GRUPO
   Añade un grupo del sistema

adduser USUARIO GRUPO
   Añade un usuario existente a un grupo existente


opciones generales:
  --quiet | -q         no mostrar información del proceso en
                       la salida estándar
  --force-badname      permitir nombres de usuarios que no
                       coincidan con la variable de configuración
                       NAME_REGEX
  --help | -h          mensaje de uso
  --version | -v       número de versión y copyright
  --conf | -c FICHERO  usa FICHERO como fichero de configuración

root@sysadmin:/home/xeon# deluser -h    # Elimina un usuario normal del sistema
root@sysadmin:/home/xeon# delgroup -h   # Elimina un grupo normal del sistema
deluser USUARIO
  elimina un usuario normal del sistema
  ejemplo: deluser miguel

  --remove-home             elimina el directorio personal del usuario y la cola de correo.
  --remove-all-files        elimina todos los ficheros que pertenecen al usuario.
  --backup                  hace una copia de seguridad de los ficheros antes de borrar.
  --backup-to <DIR>         directorio destino para las copias de seguridad.
                            Se utiliza el directorio actual por omisión.
  --system                  sólo eliminar si es un usuario del sistema.

delgroup GRUPO
deluser --group GRUPO
  elimina un grupo del sistema
  ejemplo: deluser --group estudiantes

  --system                  sólo eliminar si es un grupo del sistema.
  --only-if-empty           sólo eliminar si no tienen más miembros.

deluser USUARIO GRUPO
  elimina al usuario del grupo
  ejemplo: deluser miguel estudiantes

opciones generales:
  --quiet | -q         no dar información de proceso en la salida estándar
```

```
  --help | -h          mensaje de uso
  --version | -v       número de versión y copyright
  --conf | -c FICHERO  usa FICHERO como fichero de configuración
```

Políticas

Existen dos tipos de políticas que debemos considerar al crear las cuentas de usuarios:

- Políticas de Cuentas de Usuarios
- Políticas de envejecimiento de las contraseñas

Políticas de Cuentas de Usuarios

En la práctica, los componentes fundamentales que identifican a una cuenta de usuario son:

- Nombre de la cuenta del usuario - user *LOGIN*, que no el nombre y los apellidos.
- Id del usuario - *UID*.
- Grupo principal al cual pertenece - *GID*.
- Contraseña - *password*.
- permisos de acceso - *access permissions*.

Los principales factores a considerar durante la creación de una cuenta de usuarios son:

- La magnitud de tiempo durante el cual el usuario tendrá acceso al sistema de archivos y recursos.
- La magnitud de tiempo en que el usuario debe cambiar su contraseña -de forma periódica- por razones de seguridad.
- La magnitud de tiempo que el inicio de sesión -login- permanecerá activo.

Además, al asignar a un usuario su *UID* y *password*, debemos tener en cuenta que:

- El valor entero *UID* debe ser único y no negativo.
- El *password* debe tener una adecuada longitud y complejidad, de forma que sea difícil descifrarla.

Políticas de envejecimiento de contraseñas

En un sistema Linux, el *password* de un usuario no tiene asignado un tiempo de expiración por defecto. Si utilizamos las políticas de envejecimiento de las contraseñas, podemos cambiar el comportamiento por defecto y al crear usuarios se tomarán en cuenta las políticas definidas.

En la práctica, son dos los factores a considerar cuando establecemos la edad de una contraseña:

- Seguridad.
- Conveniencia del usuario.

Una contraseña es mas segura mientras mas corto sea su período de expiración. Se corre menos riesgo de que se filtre a otros usuarios.

Para establecer las políticas de envejecimiento de las contraseñas, podemos utilizar el comando ***chage***:

```
[root@linuxbox ~]# chage
Modo de uso: chage [opciones] USUARIO

Opciones:
  -d, --lastday ÚLTIMO_DÍA      establece el día del último cambio de la
                                contraseña a ÚLTIMO_DÍA
  -E, --expiredate FECHA_CAD    establece la fecha de caducidad a FECHA_CAD
  -h, --help                    muestra este mensaje de ayuda y termina
  -I, --inactive INACTIVA       deshabilita la cuenta después de INACTIVA
                                días de la fecha de caducidad
  -l, --list                    muestra la información de la edad de la cuenta
  -m, --mindays DÍAS_MIN        establece el número mínimo de días antes de
                                cambiar la contraseña a DÍAS_MIN
  -M, --maxdays DÍAS_MAX        establece el número máximo de días antes de
                                cambiar la contraseña a DÍAS_MAX
  -R, --root CHROOT_DIR         directory to chroot into
```

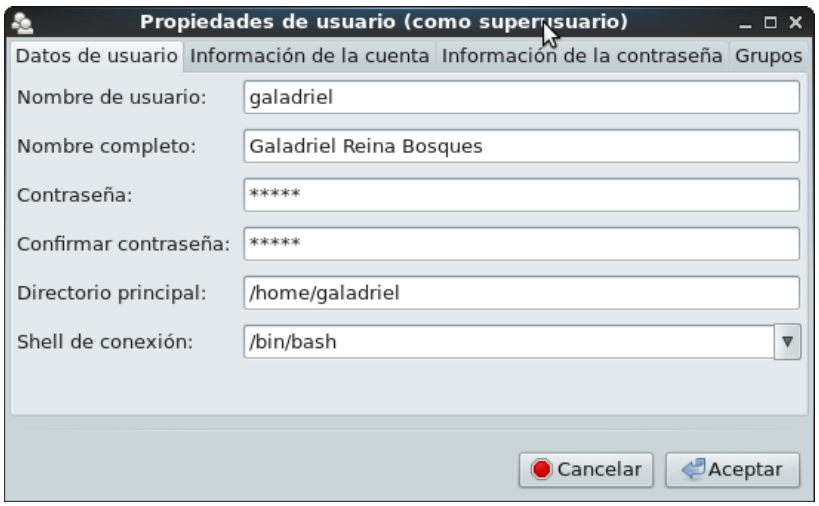
```
  -W, --warndays DÍAS_AVISO     establece los días de aviso de expiración a
                                DÍAS_AVISO
```

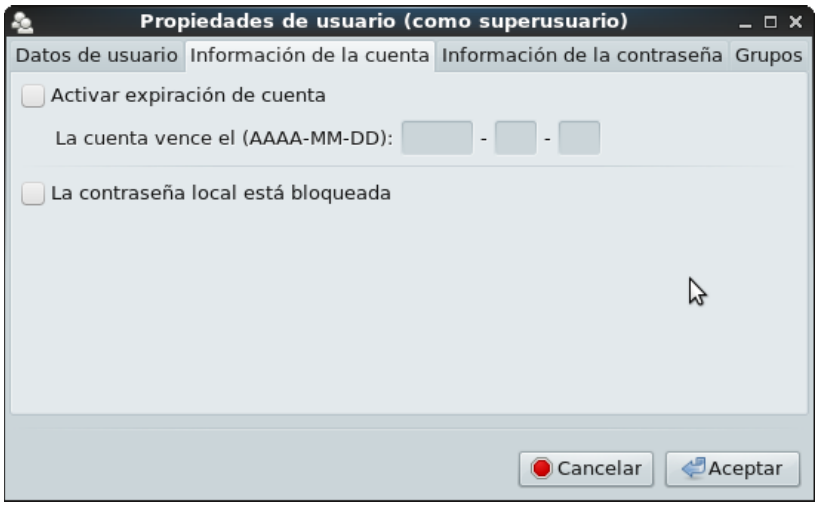
En el artículo anterior creamos varios usuarios como ejemplo. Si queremos saber los valores de la edad de la cuenta del usuario con *LOGIN* **galadriel**:

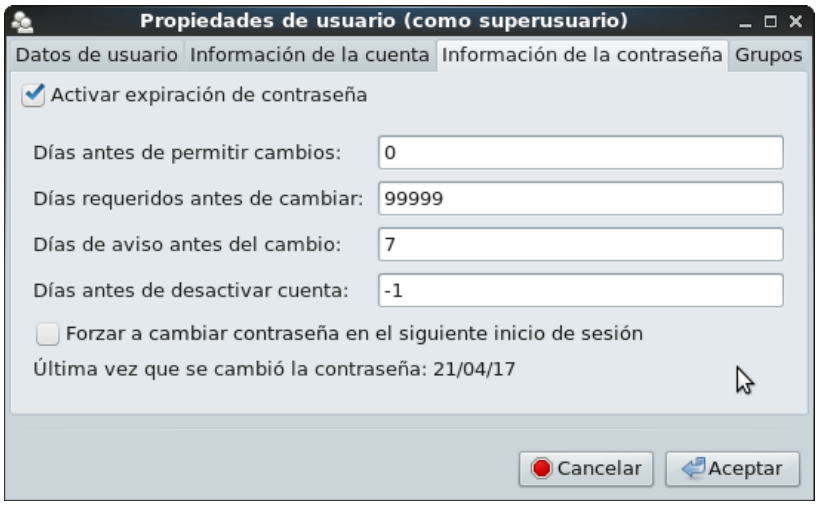
```
[root@linuxbox ~]# chage --list galadriel
Último cambio de contraseña                             :abr 21, 2017
La contraseña caduca                                    : nunca
Contraseña inactiva                                     : nunca
La cuenta caduca                                        : nunca
Número de días mínimo entre cambio de contraseña        : 0
Número de días máximo entre cambio de contraseña        : 99999
Número de días de aviso antes de que caduque la contraseña      : 7
```

Esos fueron los valores por defecto que el sistema tenía cuando creamos la cuenta de usuario mediante la utilidad gráfica de administración de "Usuarios y grupos":

Nombre de usuario	ID de usuario	Grupo principal	Nombre completo	Shell de conexión	Directorio principal
bilbo	1009	bilbo	Bilbo Bagins	/bin/bash	/home/bilbo
buzz	1000	buzz	Buzz	/bin/bash	/home/buzz
elrond	1008	elrond	Elrond Rey Elfo	/bin/bash	/home/elrond
frodo	1010	frodo	Frodo Bagins	/bin/bash	/home/frodo
galadriel	1005	galadriel	Galadriel Reina Bosques	/bin/bash	/home/galadriel
gandalf	1004	gandalf	Gandalf Mago	/bin/bash	/home/gandalf
gimly	1003	gimly	Gimly Enano	/bin/bash	/home/gimly
legolas	1002	legolas	Legolas Arquero	/bin/bash	/home/legolas
meriadoc	1007	meriadoc	Meriadoc Tuk	/bin/bash	/home/meriadoc
pipin	1006	pipin	Pipin Tuk	/bin/bash	/home/pipin
samsagaz	1011	samsagaz	Sam Sagaz	/bin/bash	/home/samsagaz
trancos	1001	trancos	Trancos Rey	/bin/bash	/home/trancos







Para cambiar los valores por defecto del envejecimiento de las contraseñas, se recomienda editar el archivo ***/etc/login.defs*** y *modificar la cantidad mínima de valores que necesitemos*. En ese archivo solo cambiaremos los valores siguientes:

```
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999   # !mas de 273 años!
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
```

por los valores que escogimos acorde a nuestro criterio y necesidades:

```
PASS_MAX_DAYS   42      # 42 días continuos que se puede usar el password
PASS_MIN_DAYS   0       # la contraseña se puede cambiar en cualquier momento
PASS_MIN_LEN    8       # longitud mínima de la contraseña
PASS_WARN_AGE   7       # Cantidad de días en que el sistema te advierte que
                        # debes cambiar la contraseña antes de que expire.
```

El resto del archivo lo dejamos tal y como estaba y recomendamos no cambiar otros parámetros hasta que no sepamos bien que estamos haciendo.

Los nuevos valores se tomarán en cuenta cuando creemos nuevos usuarios. Si cambiamos la contraseña de un usuario ya creado, se respetará el valor de la longitud mínima de la contraseña. Si utilizamos el comando ***passwd*** en vez de la utilidad gráfica y escribimos que la contraseña será "*legolas17*", el sistema se queja al igual que la herramienta gráfica "Usuarios y grupos" y nos responde que "*De alguna manera, en la contraseña se lee el nombre del usuario*" aunque al final acepte esa débil contraseña.

```
[root@linuxbox ~]# passwd legolas
Cambiando la contraseña del usuario legolas.
Nueva contraseña: arquero                               # tiene menos de 7 caracteres
CONTRASEÑA INCORRECTA: La contraseña tiene menos de 8 caracteres
Vuelva a escribir la nueva contraseña: legolas17
Las contraseñas no coinciden.                           # Lógico ¿no?
Nueva contraseña: legolas17
CONTRASEÑA INCORRECTA: De alguna manera, en la contraseña se lee el nombre del usuario
Vuelva a escribir la nueva contraseña: legolas17
passwd: todos los símbolos de autenticación se actualizaron con éxito.
```

Incurrimos en "la debilidad" de declarar una contraseña que incluye el *LOGIN* del usuario. Esa es una práctica no recomendada. Lo correcto sería:

```
[root@linuxbox ~]# passwd legolas
Cambiando la contraseña del usuario legolas.
Nueva contraseña: AltosMontes01
Vuelva a escribir la nueva contraseña: AltosMontes01
passwd: todos los símbolos de autenticación se actualizaron con éxito.
```

Para cambiar los valores de expiración del *password* de *galadriel*, hacemos uso del comando chage, y solamente debemos cambiar el valor de *PASS_MAX_DAYS* de 99999 a 42:

```
[root@linuxbox ~]# chage -M 42 galadriel
[root@linuxbox ~]# chage -l galadriel
Último cambio de contraseña                             :abr 21, 2017
La contraseña caduca                                    : jun 02, 2017
Contraseña inactiva                                     : nunca
La cuenta caduca                                        : nunca
Número de días mínimo entre cambio de contraseña        : 0
Número de días máximo entre cambio de contraseña        : 42
Número de días de aviso antes de que caduque la contraseña      : 7
```

Y así sucesivamente, podemos cambiar las contraseñas de los usuarios ya creados y sus valores de expiración de forma manual, mediante la herramienta gráfica "Usuarios y grupos", o mediante un guión - *script* que automatice parte del trabajo que no sea interactivo.

- ***De esta forma, si creamos los usuarios locales del sistema de forma no recomendada por las prácticas mas comunes con respecto a la seguridad, podemos cambiar ese comportamiento antes de continuar implementando mas servicios basados en PAM***.

Si creamos el usuario *anduin* con *LOGIN* "*anduin*" y contraseña "*ElPassword*" obtendremos el siguiente resultado:

```
[root@linuxbox ~]# useradd anduin
[root@linuxbox ~]# passwd anduin
Cambiando la contraseña del usuario anduin.
Nueva contraseña: ElPassword
CONTRASEÑA INCORRECTA: La contraseña no supera la verificación de diccionario - Está basada en una palabra del diccionario.
Vuelva a escribir la nueva contraseña: ElPassword
passwd: todos los símbolos de autenticación se actualizaron con éxito.
```

O sea, que el sistema es lo suficientemente creativo para indicarnos las debilidades de un password.

```
[root@linuxbox ~]# passwd anduin
Cambiando la contraseña del usuario anduin.
Nueva contraseña: AltosMontes02
Vuelva a escribir la nueva contraseña: AltosMontes02
passwd: todos los símbolos de autenticación se actualizaron con éxito.
```

Resumen sobre las Políticas

- Es evidente que la política de complejidad de las contraseñas, así como la de una longitud mínima de 5 caracteres, está habilitada por defecto en CentOS. En Debian, la comprobación de la complejidad funciona para los usuarios normales cuando éstos tratan de cambiar su contraseña invocando el comando ***passwd***. Para el usuario *root*, no existen limitaciones por defecto.
- Es importante conocer las diferentes opciones que podemos declarar en el archivo */etc/login.defs* mediante el comando ***man login.defs***.
- También, revisar el contenido de los archivos */etc/default/useradd*, y además en Debian */etc/adduser.conf*.

Usuarios y Grupos del Sistema

En el proceso de instalación del sistema operativo se crean toda una serie de usuarios y grupos que, una literatura denomina Usuarios Estándares y otra Usuarios del Sistema. Nosotros preferimos llamarlos Usuarios y Grupos del Sistema.

Como regla, los usuarios del sistema tienen un *UID < 1000* y sus cuentas se utilizan por diferentes aplicaciones del sistema operativo. Por ejemplo, la cuenta de usuario "*squid*" es utilizada por el programa Squid, mientras que la cuenta "lp" se utiliza para el proceso de impresión desde editores de palabras o de texto.

Si queremos listar a esos usuarios y grupos, lo podemos hacer mediante los comandos:

```
[root@linuxbox ~]# cat /etc/passwd
[root@linuxbox ~]# cat /etc/group
```

Para nada es recomendable modificar a los usuarios y grupos del sistema. ;-)

Por su importancia, repetimos que en CentOS, FreeBSD, y otros sistemas operativos, se crea el grupo -del sistema- ***wheel*** para permitir el acceso como *root* solamente a los usuarios del sistema que pertenezcan a ese grupo. Lea */usr/share/doc/pam-1.1.8/html/Linux-PAM_SAG.html*, y */usr/share/doc/pam-1.1.8/html/Linux-PAM_SAG.html*. Debian no incorpora un grupo *wheel*.

Gestionando las cuentas de usuarios y grupos

La mejor forma de aprender a gestionar las cuentas de usuarios y de grupos es:

- Practicando el uso de los comandos listados anteriormente, preferentemente en una máquina virtual y *antes* de utilizar herramientas gráficas.
- Consultando los manuales o *man pages* de cada comando antes de buscar cualquier otra información en Internet.

La práctica es el mejor criterio de la verdad.

Resumen

Por mucho, un sólo artículo dedicado a la Administración de usuarios y grupos locales no es suficiente. Dependerá del interés personal en aprender y profundizar sobre éste y otros temas relacionados, el grado de conocimiento que adquiera cada Administrador. Sucede igual que con todos los aspectos que hemos desarrollado en la serie de artículos Redes PYMES.

Próxima entrega

Continuaremos implementado servicios con autenticación frente a usuarios locales. Instalaremos, entonces, un servicio de mensajería instantánea basado en el programa **Prosody**.

¡Hasta pronto!