|  |
| --- |
|  |
| MOD369 - UD8 |
|  |
| Administración Avanzada de perfiles de usuarios y perfiles de contraseña |

**[Escriba el nombre de la compañía]**

[Seleccionar fecha]

Autor: Xabier

Administración Avanzada du usuarios y perfiles de con

Administración Avanzada de perfiles de usuarios y perfiles de contraseña

Contenido

[/etc/shadow 1](#_Toc478057802)

[Cuestas del Sistema 3](#_Toc478057803)

[Creación de cuentas de usuario: 5](#_Toc478057804)

[Plantilla de archivos de inicialización para nuevos usuarios 7](#_Toc478057805)

[Modificar el password 8](#_Toc478057806)

[Nuevos valores predeterminados del usuario 10](#_Toc478057807)

[Bloqueo de cuentas de usuario 10](#_Toc478057808)

[Políticas de Contraseña 11](#_Toc478057809)

[Forzar a los usuarios a cambiar las contraseñas periódicamente 11](#_Toc478057810)

[Proporcionando advertencias y permitiendo que Grace se inicie 12](#_Toc478057811)

[Establecer una fecha de Caducidad 12](#_Toc478057812)

[Cómo ver las políticas de Caducidad de las contraseñas 13](#_Toc478057813)

[Ejemplo práctico 14](#_Toc478057814)

# /etc/shadow

/etc/shadow contiene la contraseña cifrada del usuario y algunos parámetros relacionados con la seguridad de la contraseña.

Además de proporcionar al administrador la capacidad de establecer los campos de caducidad de la contraseña.

Sólo el usuario root puede ver el archivo / etc / shadow. -> Los usuarios normales no pueden ver ni la contraseña cifrada.

**root@localhost:~#** tail /etc/shadow

ftp:\*:15980:0:99999:7:::

nobody:\*:15980:0:99999:7:::

vcsa:!!:16406::::::

saslauth:!!:16413::::::

postfix:!!:16413::::::

sshd:!!:16413::::::

mysql:!!:16413::::::

dbus:!!:16413::::::

ntp:!!:16413::::::

sysadmin:$6$trs.W5GR$sgPBwHSIR6Zfcw7oe05mrmtR3slZQRDur02NZ71OmZ7Uaz0Xrl0ME7tdMC1Y9rrX5Jlh1zASnXFCuYFgNHzU/0:16413:0:99999:7:::

Cada registro en /etc/shadow contiene los siguientes ocho campos, separados por dos puntos:

loginID:password:lastchg:min:max:warn:inactive:expire

| **Field** | **Example** | | **Significance** |
| --- | --- | --- | --- |
| Username | sysadmin | | Nombre de usuario |
| Password | $6$trs.W5GR$sgPBwHSIR6Zfcw7oe05mr  mtR3slZQRDur02NZ71OmZ7Uaz0Xrl0ME  7tdMC1Y9rrX5Jlh1zASnXFCuYFgNHzU/0 | | contraseña encriptada.  Nota: Un campo vacío indica que no se requiere una contraseña para iniciar sesión.  Un asterisco \*marca o signo de exclamación !indica una cuenta inaccesible (por lo general del sistema) sin contraseña.  Un campo de contraseña que comienza con !seguido de la contraseña encriptada, indica la contraseña está bloqueada. |
| Last password change | | 16413 | El número de días entre el 1 de enero de 1970, y el último cambio de contraseña |
| Minimum | 0 | | número mínimo de días que la contraseña actual se pueden cambiar por el usuario |
| Maximum | 99999 | | El número máximo de días que quedan para la contraseña para que caduque; |
| Warn | 7 | | Número de días antes de la caducidad de la contraseña que el usuario es avisado |
| Inactive | 30 | | Number of days after password expiry that the user account remains active |
| Expire | 17000 | | Fecha que indica cuándo se eliminará la contraseña y el usuario quedará inactivo |
| Reserved field |  | | reservado para uso futuro |

# Cuestas del Sistema

Como presentado anteriormente, los sistemas Linux vienen con las cuentas del sistema para fines especiales root, ssh, ftp, mail, news y otros usuarios del sistema. Estas cuentas se definen en /etc/passwd..

**sysadmin@localhost:~$** cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

adm:x:3:4:adm:/var/adm:/sbin/nologin

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin

operator:x:11:0:operator:/root:/sbin/nologin

games:x:12:100:games:/usr/games:/sbin/nologin

gopher:x:13:30:gopher:/var/gopher:/sbin/nologin

ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin

nobody:x:99:99:Nobody:/:/sbin/nologin

vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin

saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin

postfix:x:89:89::/var/spool/postfix:/sbin/nologin

sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin

...

Estas cuentas se utilizan para los servicios que se ejecutan, que están estrechamente vinculados con un conjunto específico de los programas o aplicaciones.

Las cuentas del sistema se gestionan usuario root o admin group.

En los sistemas operativos tradicionales de Unix, las cuentas con números de UID menores a  100 reservados para las cuentas del sistema.

En las distribuciones de Linux basadas en RedHat, el rango reservado de cuentas del sistema es de 0- 499.

En las distribuciones de Linux basadas en Debian, ese rango se ha aumentado hasta 999.

El /etc/logins.def contiene la configuración que permite al administrador especificar qué el número mínimo de los usuario normales:

**sysadmin@localhost:~$** cat /etc/login.defs | grep UID

UID\_MIN 1000

UID\_MAX 60000

#SYS\_UID\_MIN 100

#SYS\_UID\_MAX 999

| **Parameter** | **Type** | **Meaning** |
| --- | --- | --- |
| UID\_MAX | number | Maximum number of the UID range |
| UID\_MIN | number | Minimum number of the UID range |

The UID number is automatically increased by one each time additional new user accounts are created.

Este concepto también se utiliza para los grupos

**sysadmin@localhost:~$** cat /etc/login.defs | grep GID

GID\_MIN 1000

GID\_MAX 60000

#SYS\_GID\_MIN 100

#SYS\_GID\_MAX 999

| **Parameter** | **Type** | **Meaning** |
| --- | --- | --- |
| GID\_MAX | number | Maximum number of the GID range |
| GID\_MIN | number | Minimum number of the GID range |

# Creación de cuentas de usuario:

Es un proceso de dos pasos:

1. Crear la nueva cuenta
2. Establecer una contraseña para la cuenta.

 useradd se utiliza para crear una nueva cuenta de usuario. Para añadir un nuevo usuario llamado test\_user, ejecute el siguiente comando como root:

**root@localhost:~#** useradd test\_user

Para comprobar si el comando se ha realizado correctamente, utilice la tail -1 en /etc/passwd y /etc/shadow:

**root@localhost:~#** tail -1 /etc/passwd

test\_user:x:1003:1003::/home/test\_user:

**root@localhost:~#** tail -1 /etc/shadow

test\_user:!:16455:0:99999:7:::

Observe que el campo contraseña en /etc/shadow se establece en !, lo que significa que la cuenta está bloqueada por defecto. Utilice el passwd para asignar una contraseña para la nueva cuenta de usuario:

**root@localhost:~#** passwd test\_user

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

**Observaciones**

En el ejemplo anterior no se han utilizado opciones con el comando useradd.

Este utiliza las opciones por defecto y del archivo de configuración /etc/logins.def

. Para ver las opciones por defecto utilizadas para la creación de la cuenta,

 Useradd –D:

**root@localhost:~#** useradd -D

GROUP=100

HOME=/home

INACTIVE=-1

EXPIRE=

SHELL=/bin/sh

SKEL=/etc/skel

CREATE\_MAIL\_SPOOL=no

Las opciones por defecto se establecen en  /etc/default/useradd .

**root@localhost:~#** useradd -D -s /bin/bash

GROUP=100

HOME=/home

INACTIVE=-1

EXPIRE=

SHELL=/bin/bash

SKEL=/etc/skel

CREATE\_MAIL\_SPOOL=no

Para crear un nuevo usuario con opciones diferentes a los valores por defecto, utilice useradd con parámetros opcionales:

useradd -s <Shell> -d <Home directory> -m -k <Skeleton directory> -g <Group> username

| **Option** | **Meaning** |
| --- | --- |
| -s | Shell por defecto del nuevo usuario  The default on most Linux systems is /bin/bash.  Other popular alternatives are: /bin/tsh, /bin/dash, /bin/zsh, and /bin/ksh. |
| -d | Directorio home del nuevo usuario.  The default on most Linux systems is /home/username. |
| -m | Crea el directorio home del usuario si no se ha creado. |
| -k | Copia los ficheros de inicialización del lugar especificado.  The default is /etc/skel. |
| -g | Nombre de grupo.  The default group varies depending on the Linux distribution. |
| -N | Evita la creación de un grupo con el mismo nombre del usuario.  An alternative group should be specified with the –g option. |

**root@localhost:~#** useradd -s /bin/dash -d /home/qa\_user1 -m -g netdev qa\_user1

**root@localhost:~#** tail -1 /etc/passwd

qa\_user1:x:1004:103::/home/qa\_user1:/bin/bash

**root@localhost:~#** tail -1 /etc/shadow

qa\_user1:!:16455:0:99999:7:::

**root@localhost:~#** grep netdev /etc/group

netdev:x:102:

# Plantilla de archivos de inicialización para nuevos usuarios

/etc/skel contiene el conjunto predeterminado de archivos "esqueleto" (plantilla) y directorios, que se copian en el directorio principal de un usuario que se crea con  useradd.

Esto proporciona una estructura de directorios uniforme para todos los nuevos usuarios del sistema.

Si el administrador desea hacer un cambio en la estructura de directorios o un archivo de contenido, entonces el /etc/skel asegura que el cambio se propagará a todos los nuevos usuarios.

Notas importantes:

* El /etc/skel sólo se utiliza para propagar las cuentas cuando se crea una cuenta.
* Después de que los archivos se copian en los directorios de inicio del usuario, la propiedad de estos nuevos archivos se cambiará a la nueva cuenta de usuario.
* Esto significa que un usuario puede modificar el contenido de estos archivos, ya que son propiedad del usuario.
* Algunos de los archivos que se encuentran comúnmente en este directorio son:
  + .bashrc - Contiene las definiciones de alias, permite las funciones de shell, etc.
  + .profile - Contiene definiciones de variables y comandos para configurar el entorno del usuario
  + .bash\_logout - Contiene las acciones a realizar cuando cierra la sesión

Por lo general, un administrador usará el /etc/skel sirve para generar un entorno personalizado para las nuevas cuentas de usuario.

Es posible crear diferentes skel para los diferentes tipos de cuentas de usuario.

 Por ejemplo, considere una situación que requiere diferentes archivos de personalización para tres grupos de usuarios:

developers, sales y  admin. Crear tres directorios diferentes (por ejemplo /etc/skel\_dev, /etc/skel\_sales y /etc/skel\_admin y poblar cada directorio con diferentes archivos de personalización.

 A continuación, especifique el directorio de plantilla con –k para el comando  useradd.

 El ejemplo siguiente se crea el nuevo usuario  dan con la estructura de directorios copiados de /etc/skel\_dev:

**root@localhost:~#** useradd -k /etc/skel\_dev dan

# Modificar el password

 passwd se utiliza para actualizar la contraseña de un usuario. Los usuarios sólo pueden cambiar sus propias contraseñas, mientras que el usuario root puede actualizar la contraseña de cualquier usuario.

**sysadmin@localhost:~$** passwd

Changing password for sysadmin.

(current) UNIX password:

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Si el usuario root quiere modificar el password ejecutará:

**root@localhost:~#** passwd sysadmin

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

Si el usuario desea ver el status de su password

**sysadmin@localhost:~$** passwd -S sysadmin

sysadmin P 03/01/2015 0 99999 7 -1

| **Field** | **Example** | **Meaning** |
| --- | --- | --- |
| User Name | sysadmin | Nombre de usuario |
| Password status | P | P password utilizable”  L password bloqueado  NP no password |
| Last password change date | 03/01/2015 | Ultima modificación del password |
| Minimum | 0 | Mínimo de días que deben pasar para poder modificar el password |
| Maximum | 99999 | Máximo de días para que el password expire |
| Warn | 7 | Number of days prior to password expiry that the user is warned |
| Inactive | -1 | Número de dóas tras la expiración del password que el usuario se mantendrá activo |

El usuario root puede provocar el cambio de pasword en el próximo inicio de sesión con el siguiente comando:

**root@localhost:~#** passwd -e sysadmin

passwd: password expiry information changed.

Esto obligará al usuario que durante el próximo inicio este tenga que cambiar la contraseña.

# Nuevos valores predeterminados del usuario

El /etc/login.defs contiene los parámetros que definen los valores predeterminados que se utilizan cuando se crean nuevas cuentas de usuario de Linux,

* Ubicación del directorio principal
* Los nuevos permisos de archivos,
* Controles de vencimiento de la contraseña, etc.

Este es un archivo de texto plano con un parámetro de configuración en cada línea.

 Hay tres tipos de parámetros: booleano (verdadero o falso),

Los tres parámetros que marcan la contraseña por defecto

| **Parámetro** | **Tipo** | **Sentido** |
| --- | --- | --- |
| PASS\_MAX\_DAYS | número | El número máximo de días que una contraseña es válida |
| PASS\_MIN\_DAYS | número | Número mínimo de días que una contraseña es válida  " |
| PASS\_WARN\_AGE | número | Número de días antes de Caducidad de la contraseña y que da mensajes de advertencia |

**Nota:** La modificación de cualquier parámetro en el /etc/login.defs sólo afecta a las nuevas cuentas de usuario.  Utilice el chage para modificar la contraseña información de expiración de contraseñas existentes.

# Bloqueo de cuentas de usuario

El usuario root puede bloquear y desbloquear la cuenta de un usuario utilizando los comandos passwd -l username y passwd -u username respectivamente.

Cuando una cuenta está /etc/shadow bloqueada, la entrada de la contraseña en el archivo se inválida añadiendo una !o !!a la contraseña cifrada.

Para desbloquear la entrada, se eliminan los caracteres !o !!.

**root@localhost:~#** grep sysadmin /etc/shadow

sysadmin:$6$XeBamxpj$FOH6w3DvcYDuXsooDb0u6hB0tCfAj0xLzNDoRlKvHAKCYoX2FAq2pxJ/X35d5U1czBQvejol9ixiAyfrxQg1/.:16413:0:99999:7:::

**root@localhost:~#** passwd -l sysadmin

passwd: password expiry information changed.

**root@localhost:~#** grep sysadmin /etc/shadow

sysadmin:!$6$XeBamxpj$FOH6w3DvcYDuXsooDb0u6hB0tCfAj0xLzNDoRlKvHAKCYoX2FAq2pxJ/X35d5U1czBQvejol9ixiAyfrxQg1/.:16413:0:99999:7:::

**root@localhost:~#** passwd -u sysadmin

passwd: password expiry information changed.

**root@localhost:~#** grep sysadmin /etc/shadow

sysadmin:$6$XeBamxpj$FOH6w3DvcYDuXsooDb0u6hB0tCfAj0xLzNDoRlKvHAKCYoX2FAq2pxJ/X35d5U1czBQvejol9ixiAyfrxQg1/.:16413:0:99999:7:::

Si el campo contraseña de /etc/shadow está vacío, quiere decir que no es necesaria ninguna contraseña para iniciar sesión en esta cuenta. Esto no se recomienda, por razones de seguridad, pero a veces se permite en sistemas que no tienen acceso a la red.

El usuario root puede eliminar la entrada de contraseña cifrada para una cuenta de usuario ejecutando el siguiente comando:

**root@localhost:~#** passwd -d sysadmin

passwd: password expiry information changed.

**root@localhost:~#** grep sysadmin /etc/shadow

**sysadmin::16413:0:99999:7:: 16413:0:99999:7**

# Políticas de Contraseña

chage se utiliza para actualizar la información relacionada con la caducidad de la contraseña. Mediante este comando, el administrador puede aplicar una directiva de cambio de contraseña y caducidad para cuentas de usuario específicas.

Este comando puede ser ejecutado por el usuario root para modificar las cuentas de usuario;

# Forzar a los usuarios a cambiar las contraseñas periódicamente

El chage se puede utilizar para cambiar el número de días entre la creación de una nueva contraseña y cuando el usuario debe cambiar la contraseña de nuevo.

Por ejemplo, para obligar test\_user a cambiar su contraseña dentro de los 90 días desde la última modificación (de lo contrario, la contraseña "caducará"), ejecute el siguiente comando.

Este comando actualizará el quinto campo para la cuenta "test\_user" en el /etc/shadow archivo:

test\_user:$6$gLAMp5rD$:16468:0:99999:7:::

**root@localhost:~#** chage -M 90 test\_user

**root@localhost:~#** !grep

grep test\_user /etc/shadow

test\_user:$6$gLAMp5rD$:16468:0:90:7:::

**Considera esto**

Al crear un límite de la frecuencia con la que un usuario necesita cambiar su contraseña, considere también establecer un período de tiempo mínimo antes de que se le permita cambiarlo nuevamente. De forma predeterminada, se permite a los usuarios cambiar inmediatamente su contraseña después de verse obligados a cambiarla y reutilizar contraseñas antiguas. Así que, si un usuario se ve obligado a cambiar su contraseña cada 90 días, pueden cambiar inmediatamente de vuelta a lo que era antes, lo que contradice el objetivo de forzar los cambios de contraseña.

Mediante el uso de la –m, es posible especificar un número mínimo de días (cuarto campo en /etc/shadow; default=0) que el usuario tendrá que esperar antes de poder cambiar su contraseña y así evitar que cambie de inmediato a su contraseña anterior:

**root@localhost:~#** grep test\_user /etc/shadow

test\_user:$6$gLAMp5rD$.lh2mLPolR0ZzRZXlBwi3VBW386/W5K6Lksemx3EjpMUZ5FPtcbVUer7mKa7skOLOPLYhNsKzzjRxoJ0CgxeZ1:16468:0:90:7:::

**root@localhost:~#** chage -m 5 test\_user

**root@localhost:~#** !grep

grep test\_user /etc/shadow

test\_user:$6$gLAMp5rD$.lh2mLPolR0ZzRZXlBwi3VBW386/W5K6Lksemx3EjpMUZ5FPtcbVUer7mKa7skOLOPLYhNsKzzjRxoJ0CgxeZ1:16468:5:90:7:::

PAM (Pluggable Authentication Module) proporciona un método para que Linux recuerde las contraseñas utilizadas anteriormente, forzando a los usuarios a crear nuevas contraseñas cada vez.

# Proporcionando advertencias y permitiendo que Grace se inicie

Si un usuario tiene un límite 90 días e intenta iniciar sesión en el día 91, la cuenta se bloqueará automáticamente. El sexto campo ( /etc/shadow advertencia ) permite a los administradores especificar cuántos días antes de que la cuenta se bloquee, se advertirá al usuario del posible bloqueo.

Tenga en cuenta que esta advertencia sólo aparece cuando el usuario inicia sesión:

Iniciar sesión : test\_user

Contraseña:

Para establecer el campo de advertencia en el /etc/shadow para un usuario, utilice la –W:

**root @ localhost : ~ #** chage -W 3 test\_user

**root @ localhost : ~ #** grep test\_user / etc / shadow

test\_user : $ 6 $ $ gLAMp5rD .lh2mLPolR0ZzRZXlBwi3VBW386 / W5K6Lksemx3EjpMUZ5FPtcbVUer7mKa7skOLOPLYhNsKzzjRxoJ0CgxeZ1: 16468: 0: 90: 3 :::

Cuando el usuario no cumple con las advertencias, se bloqueará su cuenta, lo que requiere que un administrador del sistema que lo desbloqueará.

 Para proporcionar al usuario un poco más de tiempo para cambiar la contraseña, se puede permitir un período de inicio de sesión de gracia con la –Iopción (inactiva) del chagecomando:

**Root @ localhost : ~ #** chage -I 10 test\_user

**raíz @ localhost : ~ #** grep test\_user / etc / shadow

test\_user : $ 6 $ gLAMp5rD $ .lh2mLPolR0ZzRZXlBwi3VBW386 / W5K6Lksemx3EjpMUZ5FPtcbVUer7mKa7skOLOPLYhNsKzzjRxoJ0CgxeZ1: 16468: 0: 90: 3: 10 ::

El comando anterior establece el período de inicio de sesión de gracia en 10días. Esto significa que durante el período de 10 días después de que se haya alcanzado el límite máximo de edad de la contraseña, el usuario puede iniciar sesión y se verá obligado a cambiar su contraseña durante el proceso de inicio de sesión.

# Establecer una fecha de Caducidad

Para establecer la caducidad de una cuenta de usuario a una fecha específica, utilice el chage –E (Expiración), seguido de la fecha en el YYYY-MM-DD (o el formato para su ubicación):

**root@localhost:~#** chage -E “2015-04-15” test\_user

**root@localhost:~#** grep test\_user /etc/shadow

test\_user:$6$gLAMp5rD$.lh2mLPolR0ZzRZXlBwi3VBW386/W5K6Lksemx3EjpMUZ5FPtcbVUer7mKa7skOLOPLYhNsKzzjRxoJ0CgxeZ1:16468:0:90:3:10:16540:

El comando anterior actualizará el octavo campo etc/shadow fichero para la test\_user pasa a 16540 días a partir del 1 de enero de 1970, que en este caso es el 15 de abril de 2015; El día en que la cuenta será bloqueada.

Tenga en cuenta que la cuenta no se elimina cuando se alcanza la fecha de caducidad, sino que está bloqueada para evitar que el usuario inicie sesión .

# Cómo ver las políticas de Caducidad de las contraseñas

Cualquier usuario puede ver las directivas de Caducidad de la contraseña para su propia cuenta ejecutando el comando. Por ejemplo:chage –l <own\_username>

**Sysadmin @ localhost : ~ $** chage -l sysadmin

Tenga en cuenta que un usuario sólo puede ver esta información para su propia cuenta. El administrador puede utilizar este comando para cualquier cuenta de usuario.

Esto es especialmente útil para traducir el campo de expiración a una fecha real.

**sysadmin@localhost:~$** chage -l sysadmin

Last password change : Dec 18, 2014

Password expires : never

Password inactive : never

Account expires : never

Minimum number of days between password change : 0

Maximum number of days between password change : 99999

Number of days of warning before password expires : 7

# Ejemplo práctico

PASO1

Crear usuario:

useradd joe

**root@localhost:~#** useradd joe

PASO2

El usuario no tiene password

grep joe /etc/shadow

**root@localhost:~#** grep joe /etc/shadow

joe:!:16544:0:99999:7:::

PASO3:

Asignar password

**root@localhost:~#** passwd joe

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

PASO4:

Verificar password.

**root@localhost:~#** grep joe /etc/shadow

joe:$6$hfdcKPJY$cmhxRWCuYmZXzejAcSJqH0B7qK7Hk5Myi5QMNPnxLzC9r/TFZYHrYK0YS.xd11y0

GDAtBN6sfkB5AZCFFz2Mr.:16544:0:99999:7:::

PASO5:

Bloquear cuenta de usuario:

passwd –l joe

**root@localhost:~#** passwd -l joe

passwd: password expiry information changed.

Verificar que la cuenta está bloqueada:

grep joe /etc/shadow

**root@localhost:~#** grep joe /etc/shadow

joe:!$6$hfdcKPJY$cmhxRWCuYmZXzejAcSJqH0B7qK7Hk5Myi5QMNPnxLzC9r/TFZYHrYK0YS.xd11y

0GDAtBN6sfkB5AZCFFz2Mr.:16544:0:99999:7:::

PASO5:

Desbloquear cuenta de usuario

passwd –u joe

**root@localhost:~#** passwd -u joe

passwd: password expiry information changed.

Ver desbloqueo:

grep joe /etc/shadow

**root@localhost:~#** grep joe /etc/shadow

joe:$6$hfdcKPJY$cmhxRWCuYmZXzejAcSJqH0B7qK7Hk5Myi5QMNPnxLzC9r/TFZYHrYK0YS.xd11y0

GDAtBN6sfkB5AZCFFz2Mr.:16544:0:99999:7:::

PASO6:

Eliminar la contraseña:

passwd –d joe

**root@localhost:~#** passwd -d joe

passwd: password expiry information changed.

Comprobación:

grep joe /etc/shadow

**root@localhost:~#** grep joe /etc/shadow

joe::16544:0:99999:7:::

PASO 7:

Modificar el fichero /etc/login.defs:

PASS\_MAX\_DAYS 90

PASS\_MIN\_DAYS 0

PASS\_WARN\_AGE 7

PASO8:

Crear el usuario:

useradd sue

PASO9:

Ejecutar

grep -E 'sue|joe' /etc/shadow

**root@localhost:~#** grep -E 'sue|joe' /etc/shadow

joe::16544:0:99999:7:::

sue:!:16544:0:90:7:::

PASO10:

Forzar al usuario a cambiar su contraseña de forma regular es una política de seguridad básica.

Para forzar a tim a cambiar su password cada 60 días usaremos el comando chage.

En el fichero el valor asignado es de 90 días:

grep tim /etc/shadow

**root@localhost:~#** grep tim /etc/shadow

tim:!:16544:0:90:7:::

Este valor viene de la modificación realizada anteriormente en el fichero /etc/login.defs

PASO11

Ejecutar el siguiente comando para modificar el periodo de cambio de password a 60 días.

chage -M 60 tim

grep time /etc/shadow

**root@localhost:~#** chage -M 60 tim

**root@localhost:~#** grep tim /etc/shadow

tim:!:16544:0:60:7:::

PASO12

Si en los siguientes 60 días tim no modificara su password su cuenta de usuario se bloqueará. Para que el sistema avise del cambio de contraseña utilizar la opción –W y para permitir un periodo de gracia de 15 días desde que la contraseña expiro utilizar –I:

grep tim /etc/shadow

chage -W 10 -I 15 tim

grep tim /etc/shadow

**root@localhost:~#** grep tim /etc/shadow

tim:!:16544:0:60:7:::

**root@localhost:~#** chage -W 10 -I 15 tim

**root@localhost:~#** grep tim /etc/shadow

tim:!:16544:0:60:10:15::

PASO13

Para establecer una fecha de expiración para el usuario tim:

chage -E "2014-12-12" tim

grep tim /etc/shadow

**root@localhost:~#** chage -E "2014-12-12" tim

**root@localhost:~#** grep tim /etc/shadow

tim:!:16544:0:60:10:15:16416:

PASO14

Esta fecha de expiración se representa como el número de días transcurridos desde el 1 de Enero del 1970.

Para visualizar esta información.

chage -l tim

**root@localhost:~#** chage -l tim

Last password change : Apr 19, 2015

Password expires : Jun 18, 2015

Password inactive : Jul 03, 2015

Account expires : Dec 12, 2014

Minimum number of days between password change : 0

Maximum number of days between password change : 60

Number of days of warning before password expires : 10

PASO15

Para modificar un usuario el commando será usermod :

usermod -G sysadmin tim

**root@localhost:~#** usermod -G sysadmin tim

groups tim

**root@localhost:~#** groups tim

tim : tim sysadmin

PASO16

Cambiar la Shell del usuario tim y su verificación :

grep tim /etc/passwd

usermod -s /bin/tcsh tim

grep tim /etc/passwd

**root@localhost:~#** grep tim /etc/passwd

tim:x:1004:1004::/home/tim:

**root@localhost:~#** usermod -s /bin/tcsh tim

**root@localhost:~#** grep tim /etc/passwd

tim:x:1004:1004::/home/tim:/bin/tcsh

PASO17

Para eliminar la cuenta de usuario:

userdel -r tim

grep tim /etc/passwd

**root@localhost:~#** userdel -r tim

userdel: tim mail spool (/var/mail/tim) not found

**root@localhost:~#** grep tim /etc/passwd

La opción –r eliminará también el directorio HOME y el fichero mail.