Políticas de Seguridad

Actividad 4

Cristóbal Suárez Abad
Seguridad y Alta Disponibilidad – 2º ASIR

Contenido

Intro

Sigue esta guía:

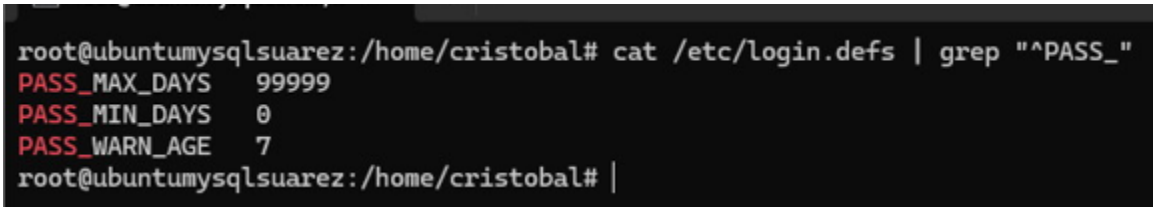
https://labex.io/es/tutorials/linux-how-to-enforce-password-complexity-policies-in-linux-414805

Añade pantallazos y explicaciones que consideres necesario.

Archivos de configuración de contraseñas.

/etc/login.defs es el archivo que contiene las configuraciones básicas de contraseñas.

cat /etc/login.defs | grep "^PASS_"



Nos muestra el número máximo de días que una contraseña se mantiene válida, el número mínimo de días requeridos entre cambios de contraseña y el número de días de advertencia antes de la expiración de la contraseña.

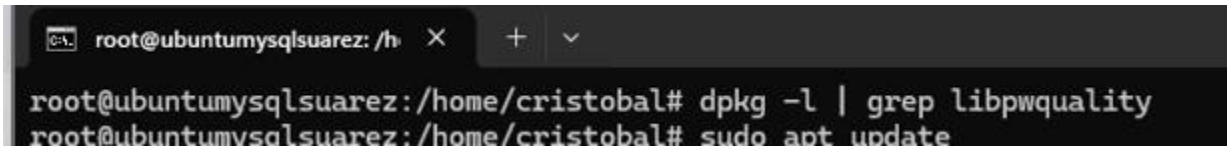
*"**/etc/pam.d/common-password**, que gestiona la configuración de PAM (Módulos de Autenticación Enchufables - Pluggable Authentication Modules) para la autenticación de contraseñas:"* El archivo se encuentra completamente comentado y en él se configuran los requisitos de complejidad de contraseñas.

cat /etc/pam.d/common-password

```
root@ubuntumysqlsuarez:/home/cristobal# cat /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure yescrypt
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
root@ubuntumysqlsuarez:/home/cristobal#
```

El sistema usa “pwaquality” para aplicar la calidad de contraseña. Podemos ver si lo tenemos instalado usando:

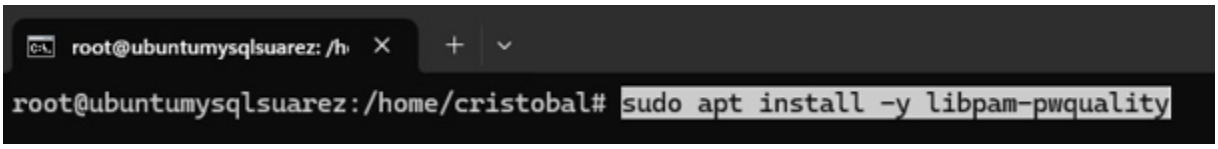
dpkg -l | grep libpwquality



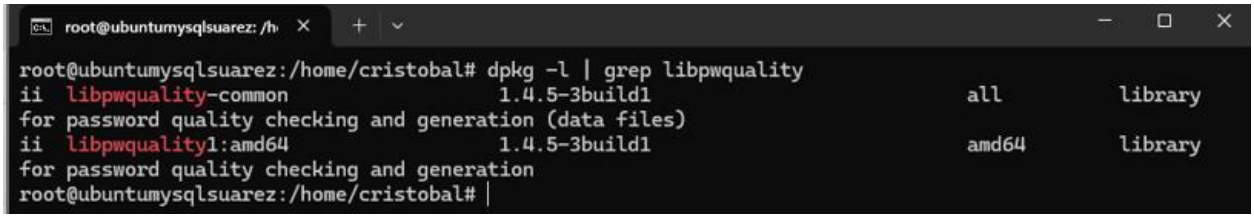
Si no aparece nada es que no lo tenemos instalado. Podemos instalarlo con:

sudo apt update

sudo apt install -y libpam-pwquality

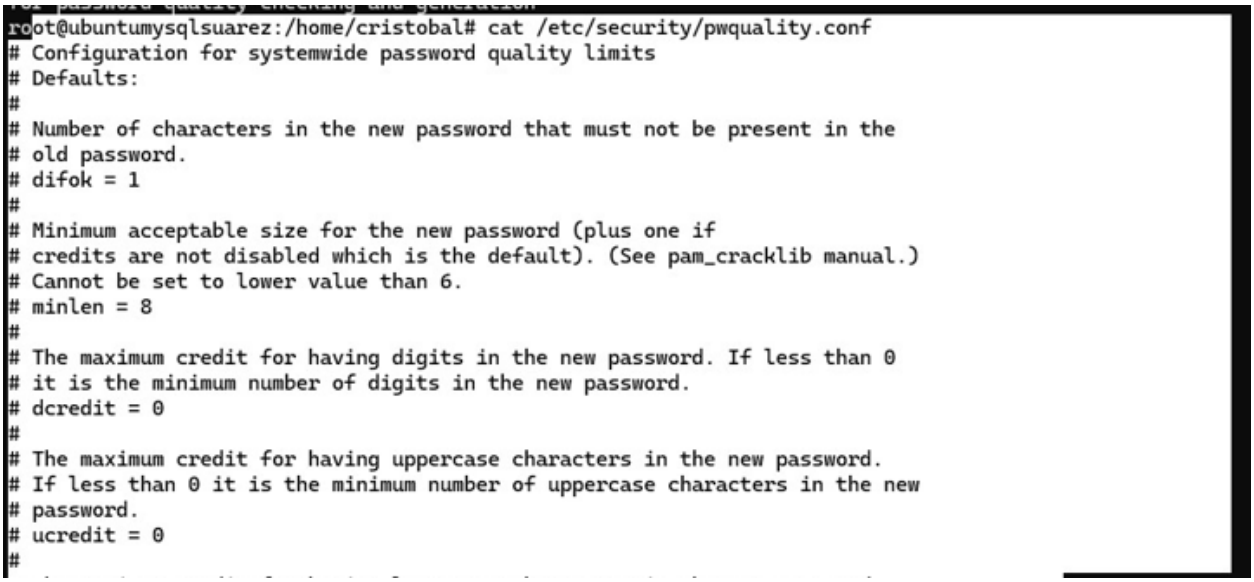


Lo comprobamos de nuevo:



Ahora podemos examinar el archive de configuración de la calidad de la contraseña:

cat /etc/security/pwquality.conf



Comprensión de los Parámetros de la Política de Contraseñas

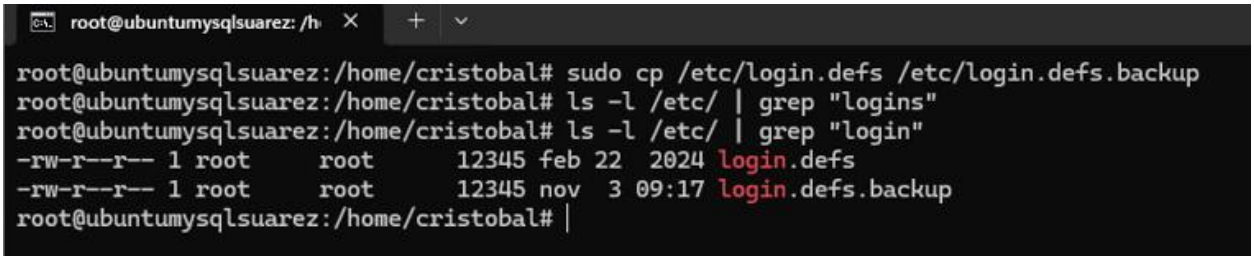
"Aquí están los parámetros clave que puede configurar:

- *minlen: Longitud mínima de la contraseña*
- *dcredit: Crédito por dígitos en la contraseña*
- *ucredit: Crédito por caracteres en mayúsculas*
- *lcredit: Crédito por caracteres en minúsculas*
- *ocredit: Crédito por caracteres especiales*
- *retry: Número de reintentos para ingresar una nueva contraseña*
- *enforce_for_root: Si se deben aplicar estas políticas al usuario root*
  Estos parámetros proporcionan un marco integral para controlar la complejidad y la seguridad de las contraseñas en su sistema Linux."

Configuración de Políticas de Contraseñas Básicas

Antes de llevar a cabo cualquier cambio, hacemos copia de seguridad:

sudo cp /etc/login.defs /etc/login.defs.backup



Abrimos el archivo: **sudo nano /etc/login.defs**

Nos dirigimos hasta las opciones que vimos previamente y le cambiamos los valores tal como se ven en la imagen.

```
# 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_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_WARN_AGE   14
```

Guardamos el archivo y comprobamos los cambios: **cat /etc/login.defs | grep "^PASS_"**

```
root@ubuntumysqlsuarez:/home/cristobal# cat /etc/login.defs | grep "^PASS_"
PASS_MAX_DAYS   90
PASS_MIN_DAYS   7
PASS_WARN_AGE   14
root@ubuntumysqlsuarez:/home/cristobal#
```

Ahora vamos a probar que la configuración se aplica a un usuario nuevo:

sudo useradd -m testuser

sudo passwd testuser

```
root@ubuntumysqlsuarez: /h
root@ubuntumysqlsuarez:/home/cristobal# sudo useradd -m testuser
root@ubuntumysqlsuarez:/home/cristobal# sudo passwd testuser
New password:
Retype new password:
passwd: password updated successfully
root@ubuntumysqlsuarez:/home/cristobal#
```

Verificamos los parámetros de la contraseña del nuevo usuario.

sudo chage -l testuser

```
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -l testuser
Last password change                                    : nov 03, 2025
Password expires                                        : feb 01, 2026
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 7
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 14
root@ubuntumysqlsuarez:/home/cristobal#
```

Configuración de los Requisitos de Complejidad de Contraseñas

Copia de seguridad:

sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.backup

```
root@ubuntumysqlsuarez:/home/cristobal# sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.
backup
root@ubuntumysqlsuarez:/home/cristobal# ls -l /etc/pam.d/ | "common-password"
common-password: command not found
root@ubuntumysqlsuarez:/home/cristobal# ls -l /etc/pam.d/ | grep "common-password"
-rw-r--r-- 1 root root 1693 nov  3 09:16 common-password
-rw-r--r-- 1 root root 1693 nov  3 09:18 common-password.backup
root@ubuntumysqlsuarez:/home/cristobal#
```

Modificamos el archivo: la línea que contenga “pam_pwquality.so”. Reemplazamos su contenido por:

password requisite pam_pwquality.so retry=3 minlen=12 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 enforce_for_root

```
# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3 minlen=12 dcredit=-1 ucred
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yesc
# here's the fallback if no module succeeds
```

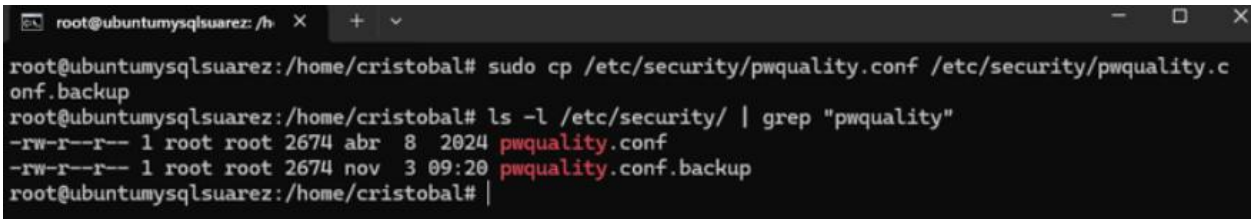
“Esta configuración significa:

- *minlen=12: La longitud mínima de la contraseña es de 12 caracteres*
- *dcredit=-1: Se requiere al menos 1 dígito*
- *ucredit=-1: Se requiere al menos 1 letra mayúscula*
- *lcredit=-1: Se requiere al menos 1 letra minúscula*
- *ocredit=-1: Se requiere al menos 1 carácter especial*
- *enforce_for_root: Aplica estas políticas también al usuario root”*

Configuración de Parámetros Adicionales en pwquality.conf

Copia de seguridad:

sudo cp /etc/security/pwquality.conf /etc/security/pwquality.conf.backup



Ahora lo configuramos de la siguiente manera:

"minlen = 12

Longitud minima acceptable (12 caracteres)

dcredit = -1

*La contraseña debe contener un **mínimo** de **1 dígito** (número). Un valor negativo indica el número mínimo requerido.*

ucredit = -1

*"uppercase" La contraseña debe contener un **mínimo** de **1 letra mayúscula**.*

lcredit = -1

*"lowercase" La contraseña debe contener un **mínimo** de **1 letra minúscula**.*

ocredit = -1

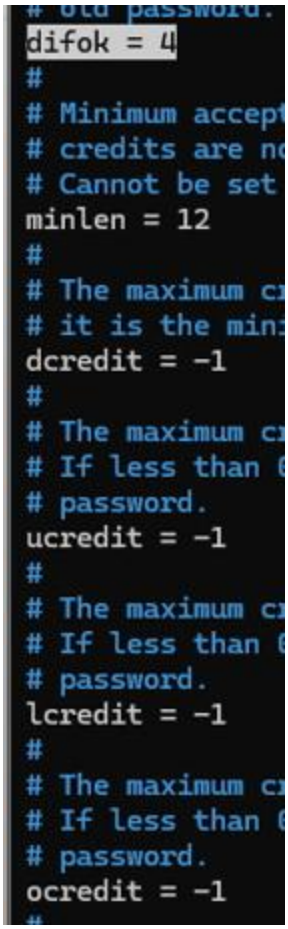
*La contraseña debe contener un **mínimo** de **1 otro carácter** (símbolo o especial).*

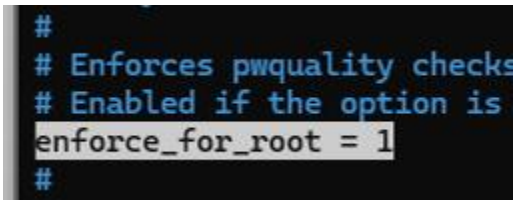
difok = 4

*El número de caracteres de la nueva contraseña que **deben ser diferentes** de la contraseña anterior es de **4**.*

enforce_for_root = 1

*La política de calidad de contraseñas se **aplica también al usuario root** (superusuario)."*


difok = 4
#
# Minimum accept
# credits are no
# Cannot be set
minlen = 12
#
# The maximum cr
# it is the mini
dcredit = -1
#
# The maximum cr
# If less than 0
# password.
ucredit = -1
#
# The maximum cr
# If less than 0
# password.
lcredit = -1
#
# The maximum cr
# If less than 0
# password.
ocredit = -1


#
# Enforces pwquality checks
# Enabled if the option is
enforce_for_root = 1
#

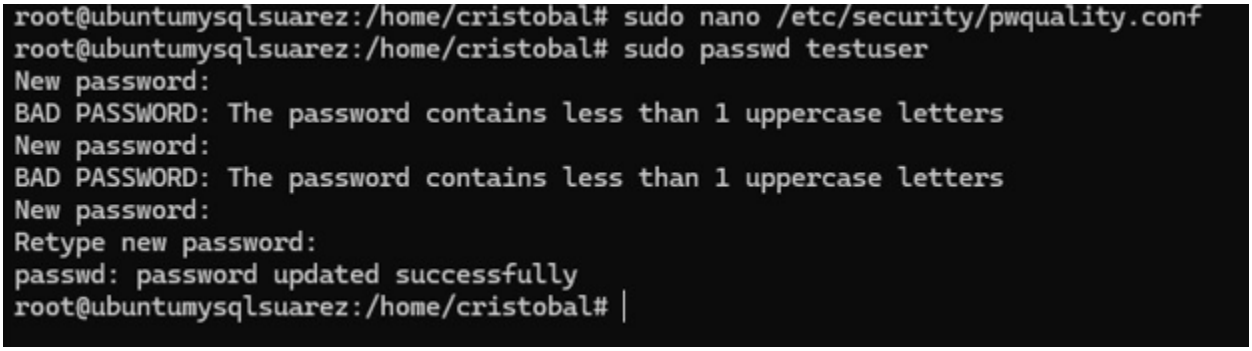
Prueba de la Nueva Política de Complejidad de Contraseñas

Vamos a intentar cambiar la contraseña del usuario de prueba por una bastante simplona:

sudo passwd testuser

password123

No se la traga. Ahora prueba con una más compleja: *Secure@Password123*. Si funciona.



Implementación de Controles de Historial de Contraseñas.

Copia de seguridad.

```
root@ubuntumysqlsuarez:/home/cristobal# sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.
backup2
root@ubuntumysqlsuarez:/home/cristobal# ls -l /etc/pam.d/ | grep "common-password"
-rw-r--r-- 1 root root 1791 nov  3 09:20 common-password
-rw-r--r-- 1 root root 1693 nov  3 09:18 common-password.backup
-rw-r--r-- 1 root root 1791 nov  3 09:24 common-password.backup2
root@ubuntumysqlsuarez:/home/cristobal#
```

Ahora lo modificamos. En la línea donde pone "**pam_unix.so**" ponemos al final un "**remember=5**". *"Esto evitará que los usuarios reutilicen cualquiera de sus 5 contraseñas más recientes." "Indica al sistema que almacene los hashes de las últimas 5 contraseñas para cada usuario",*

```
# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3 minlen=12 dcredit=-1 ucredit=-1 lcredit=-
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass sha512 remember=5
```

Guardamos.

Comprender Cómo Funciona el Historial de Contraseñas

El historial de contraseñas (los hashes que hemos mencionado antes) se guardan en "**/etc/security/opasswd**". Si no existe se creará automáticamente cuando el primer usuario cambie su contraseña.

```
root@ubuntumysqlsuarez:/home/cristobal# ls -la /etc/security/opasswd
-rw------- 1 root root 0 ago  5 16:54 /etc/security/opasswd
```

Vamos a probar la configuración anterior. Vamos a cambiar la contraseña del usuario de prueba por la misma que tiene. En teoría no debe permitirlo.

```
root@ubuntumysqlsuarez:/home/cristobal# sudo passwd testuser
New password:
Retype new password:
passwd: password updated successfully
root@ubuntumysqlsuarez:/home/cristobal#
```

Extrañamente lo permite. Esto le sucede a otros compañeros y no hemos podido llegar a una solución.

Aplicación de Políticas de Contraseñas a Usuarios Existentes

La configuración que realizamos previamente en "***/etc/login.defs***" solo se aplica a nuevos usuarios o a aquellos que cambien su contraseña. ¿Cómo podemos aplicarla a usuarios ya existentes? Primero vamos a comprobar el estado actual de la cuenta:

sudo chage -l testuser

```
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -l testuser
Last password change                                    : nov 03, 2025
Password expires                                        : feb 01, 2026
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 7
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 14
root@ubuntumysqlsuarez:/home/cristobal#
```

Si queremos obligarlo a cambiar de contraseña la próxima vez que inicie sesión usamos:

sudo chage -d 0 testuser

```
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -d 0 testuser
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -l testuser
Last password change                                    : password must be changed
Password expires                                        : password must be changed
Password inactive                                       : password must be changed
Account expires                                         : never
Minimum number of days between password change          : 7
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 14
```

"*Esto establece la fecha del último cambio de contraseña en 0, forzando un cambio de contraseña en el próximo inicio de sesión.*"

Podemos establecerla también así:

sudo chage -E $(date -d "69 days" +%Y-%m-%d) testuser

```
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -E $(date -d "69 days" +%Y-%m-%
d) testuser
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -l testuser
Last password change                                    : password must be changed
Password expires                                        : password must be changed
Password inactive                                       : password must be changed
Account expires                                         : ene 13, 2026
Minimum number of days between password change          : 7
Maximum number of days between password change          : 69
Number of days of warning before password expires       : 14
```

Establecimiento de la Antigüedad Máxima de Contraseña para Usuarios Existentes.

sudo chage -M 1492 testuser

```
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -M 1492 testuser
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -l testuser
Last password change                                    : password must be changed
Password expires                                        : password must be changed
Password inactive                                       : password must be changed
Account expires                                         : ene 13, 2026
Minimum number of days between password change          : 7
Maximum number of days between password change          : 1492
Number of days of warning before password expires       : 14
root@ubuntumysqlsuarez:/home/cristobal#
```

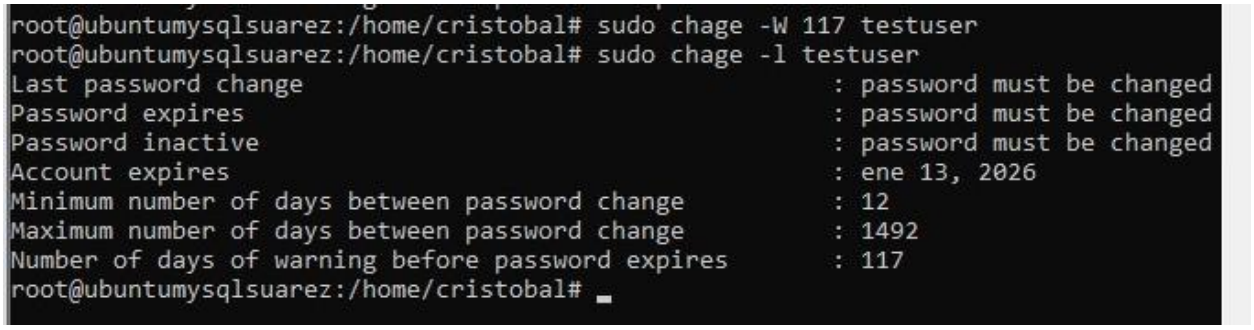
Establecimiento de la Antigüedad Mínima de Contraseña para Usuarios Existentes

sudo chage -m 12 testuser

```
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -m 12 testuser
root@ubuntumysqlsuarez:/home/cristobal# sudo chage -l testuser
Last password change                                    : password must be changed
Password expires                                        : password must be changed
Password inactive                                       : password must be changed
Account expires                                         : ene 13, 2026
Minimum number of days between password change          : 12
Maximum number of days between password change          : 1492
Number of days of warning before password expires       : 14
```

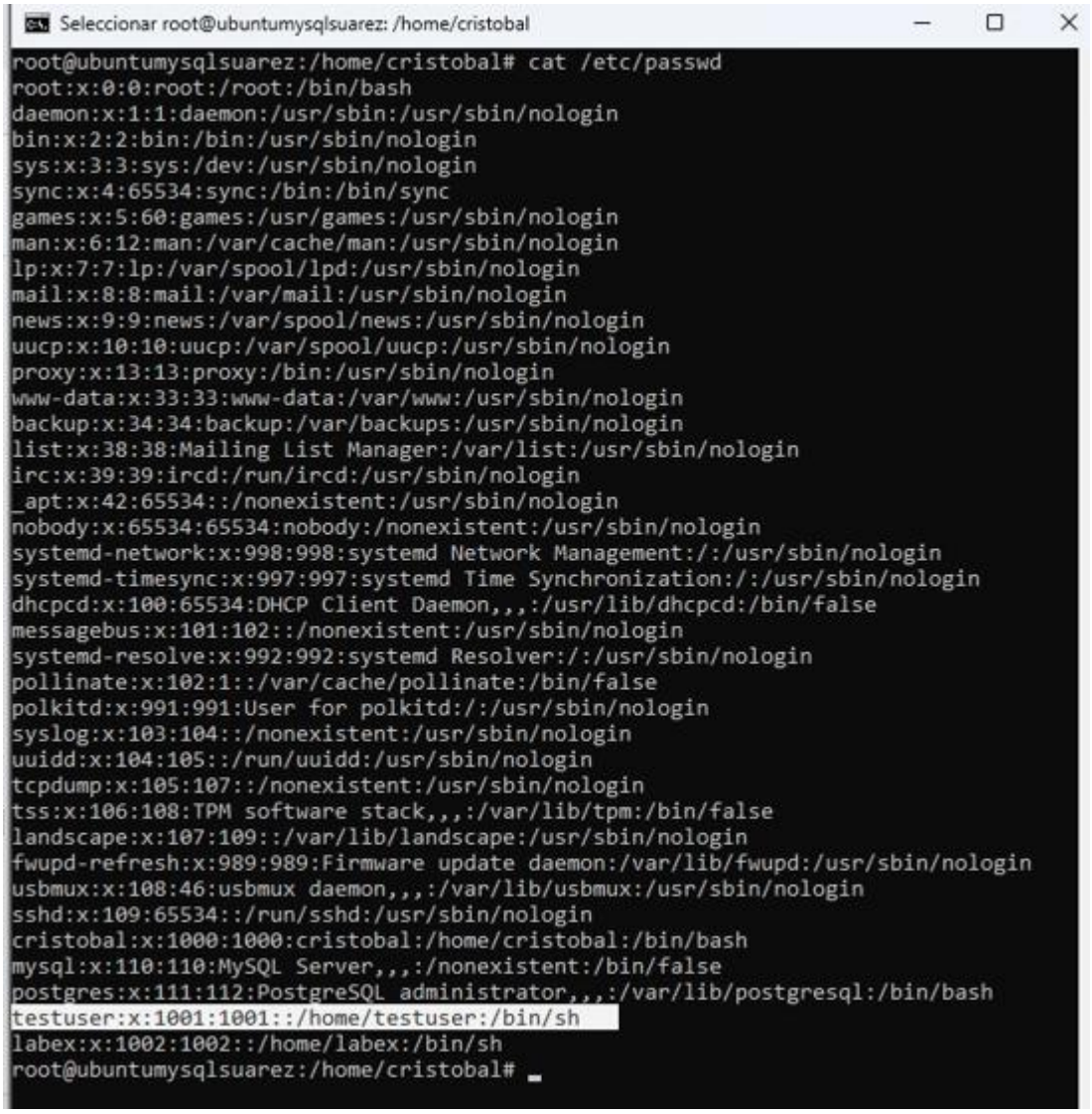
Establecimiento de la Advertencia de Expiración de Contraseña para Usuarios Existentes

sudo chage -W 117 testuser

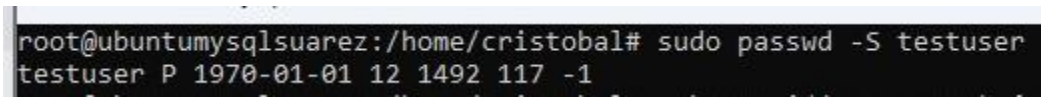


Visualización de la Información de Contraseña del Usuario

cat /etc/passwd



sudo passwd -S testuser



“Esto enumera todos los usuarios regulares en el sistema (UID >= 1000).”

awk -F: '($3 >= 1000) {print $1}' /etc/passwd

```
root@ubuntumysqlsuarez:/home/cristobal# awk -F: '($3 >= 1000) {print $1}' /etc/pas
swd
nobody
cristobal
testuser
labex
root@ubuntumysqlsuarez:/home/cristobal#
```

Aplicación de Políticas a Todos los Usuarios

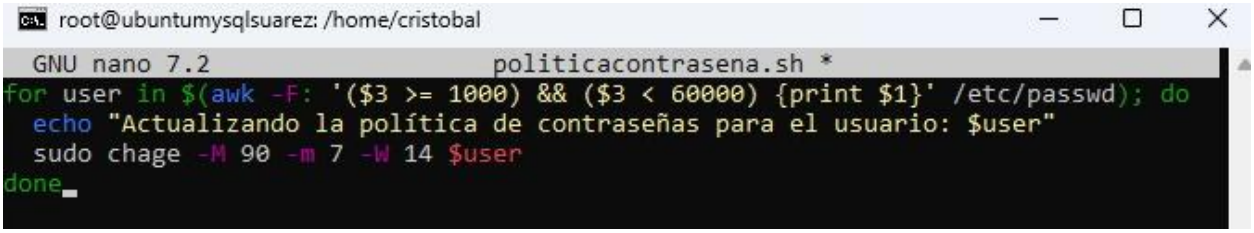
Creamos un script y le ponemos la siguiente configuración:

for user in $(awk -F: '($3 >= 1000) && ($3 < 60000) {print $1}' /etc/passwd); do

echo "Actualizando la política de contraseñas para el usuario: $user"

sudo chage -M 90 -m 7 -W 14 $user

done



Lo ejecutamos y veremos como se aplica a los usuarios:

```
root@ubuntumysqlsuarez:/home/cristobal# sh politicacontrasena.sh
Actualizando la política de contraseñas para el usuario: cristobal
Actualizando la política de contraseñas para el usuario: testuser
Actualizando la política de contraseñas para el usuario: labex
root@ubuntumysqlsuarez:/home/cristobal#
```

Este script actualiza a todos los usuarios regulares con nuestras nuevas políticas de envejecimiento de contraseñas.