10.contraseñas.odt

Autor:
Sergio López-Ventura Esteban
Email:
sergio.lopezventura@educa.madrid.org

20/10/25

Descripción

Iniciado el 20/10/2025 y finalizado el 21/10/2025

En esta practica modificaremos las políticas de contraseñas de Windows y Linux respectivamente, probaremos que funcionen y haremos algún proceso extra en Linux como creación de usuario y administración de cuotas.

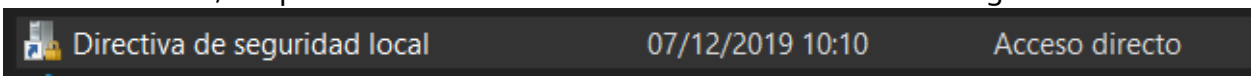
Índice

1. Windows

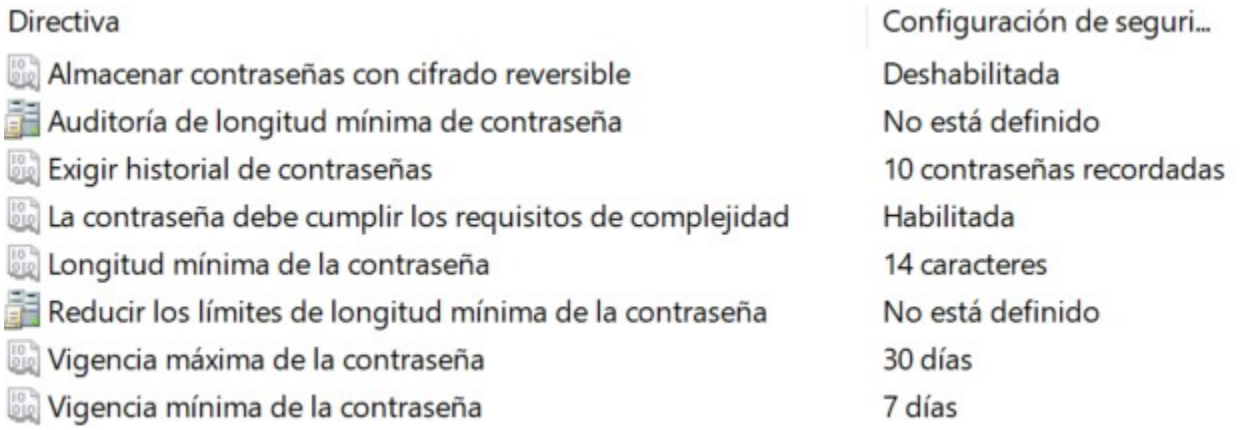
Antes de comenzar debo de aclarar que esto se hace desde un Windows 10 pro ya que en el home no existe dichas opciones. Empezaremos realizando nuestra nueva política de contraseñas, para este caso nos pide:

- 14 dígitos
- Contenga los requisitos mínimos de tipos de caracteres utilizados (minúscula, mayúscula, dígitos, carácter no alfanumérico)
- Vigencia máxima de 30 días
- Vigencia mínima de 7 días
- Tener un historial de 10 contraseñas
- Se bloquee después del quinto intento fallido de inicio de sesión
- Se desbloquee a los 2 minutos

Para cumplir todos estos requisitos iremos al panel de control y buscaremos herramientas administrativas, después de entrar seleccionaremos las directivas de seguridad local.



Justo después tendremos que dirigirnos a directivas de cuentas y directiva de contraseñas, en el menú de la parte derecha veremos variedad de opciones a habilitar, ahora modificaremos dichas opciones para acomodar nuestras políticas.

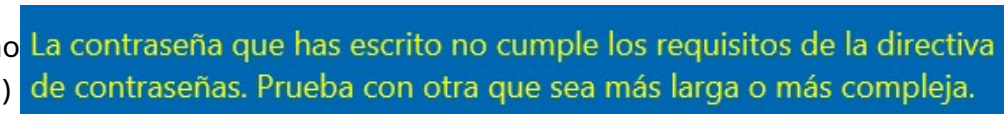


Actualmente me faltan los dos últimos requisitos, estos están justo en la pestaña de abajo "directiva de bloqueo de cuenta", los cambios se realizaron en las dos últimas directivas.

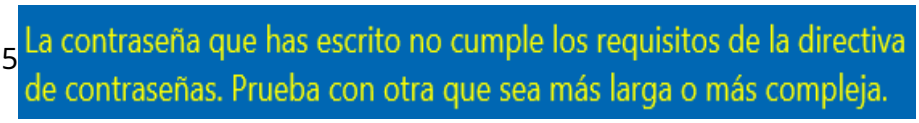
Directiva	Configuración de seguri...
Duración del bloqueo de cuenta	10 minutos
Permitir bloqueo de cuenta de administrador	Habilitada
Restablecer el bloqueo de cuenta después de	2 minutos
Umbral de bloqueo de cuenta	5 intentos de inicio de se...

Por último comprobaré dicha política, con un usuario cambiaré la contraseña para pasar por todas las condiciones:

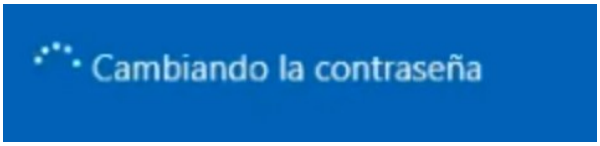
1. contraseña: alumno (no pongo mayúscula)



2. contraseña: Alumno202025 (tiene 12 caracteres)



3. contraseña: Alumno202025.24



Ahora probaré a introducir cinco contraseñas incorrectas para que se bloquee la cuenta por dos minutos, cargará un rato para después saltar al siguiente mensaje:

No especifica el tiempo pero en dos minutos me dejará iniciar sesión, dependiendo de la versión del sistema podrá saltar un mensaje distinto.

2. Linux

En esta ocasión los requisitos de contraseña son algo distintos:

- 1 dígito
- 2 minúsculas
- 1 mayúscula
- 1 carácter no alfanumérico (@,$,#)
- No coincidir con al menos 3 letras de la anterior
- La longitud de la misma debe ser 14 caracteres.
- Vigencia máxima de 30 días
- Vigencia mínima de 7 días
- Tener un historial de 10 contraseñas (remember=10)
- Bloquear al llevar a cabo 5 intentos fallidos
- Se desbloquea la cuenta a los 2 minutos.

Podremos cumplir esto gracias al servicio PAM que gestiona los métodos de autenticación en el sistema. Para empezar instalaremos una librería para poder modificar el fichero `/etc/security/pwquality.conf`. Este fichero lo utilizaremos para configurar los cambios en la propia contraseña, es decir, números, caracteres mínimos (minúsculas, mayúsculas, ...)

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt install libpam-cracklib
ubuntu@ubuntu-VirtualBox:~$ nvim /etc/security/pwquality.conf
```

En este fichero (`pwquality.conf`) retocaremos los siguientes parámetros:

```
Minlen = 14 # longitud mínima

dcredit = -1 # mínimo digitos

lcredit = -2 # mínimo minusculas

ucredit = -1 # mínimo mayúsculas

ocredit = -1 # mínimo caracteres no alfanuméricos

difok = 3 #  no councidir 3 letras con la anterior
```

Ahora tocaremos la vigencia de contraseñas en `/etc/pam.d/common-password`, buscaremos una linea que ponga password [success=1 ...] y lo sustituiremos por:

```
password [success=1 default=ignore] pam_unix.so obscure sha512 remember=10
```

Para establecer la vigencia entraremos en `/etc/login.defs` y tocaremos:

```
PASS_MAX_DAYS   30

PASS_MIN_DAYS   7
```

Ahora nos iremos a `/etc/pam.d/common-auth` y añadiremos:

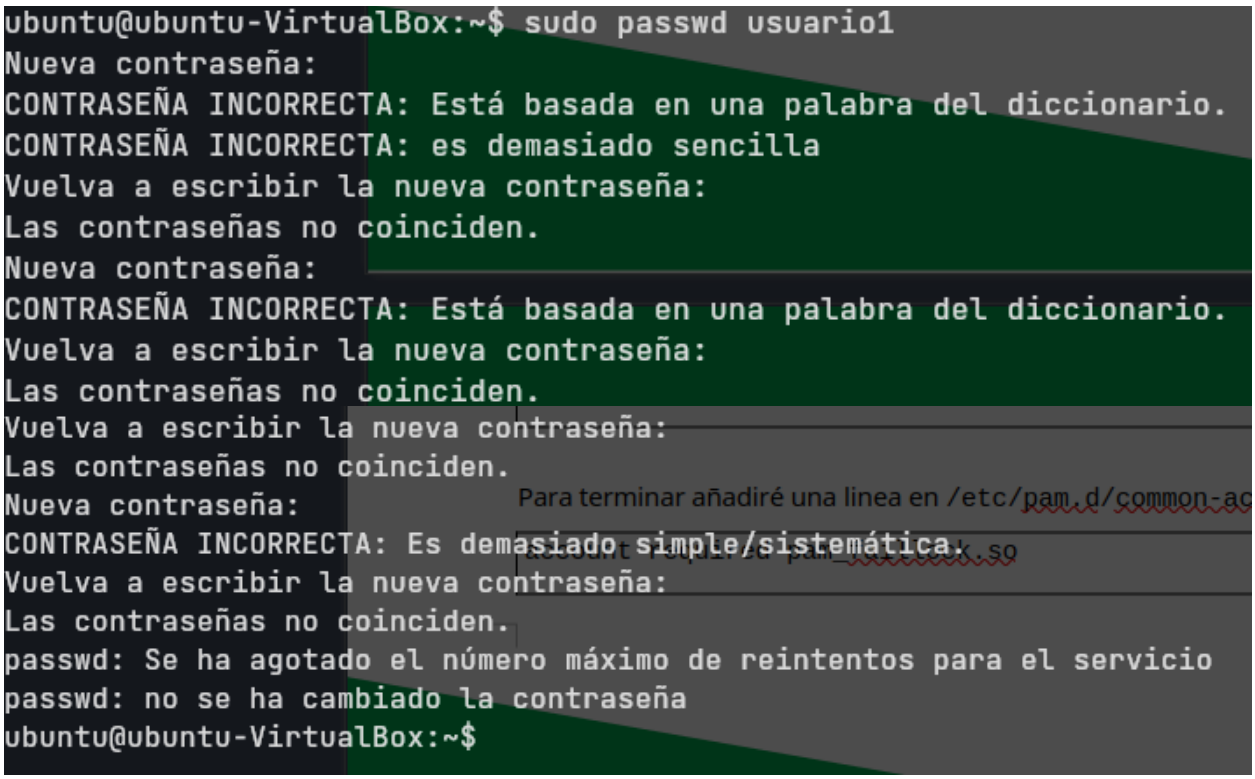
```
auth    required        pam_faillock.so preauth audit deny=5 unlock_time=120

auth    [default=die]   pam_faillock.so authfail audit deny=5 unlock_time=120
```

Para terminar añadiré una linea en `/etc/pam.d/common-account`, pondré lo siguiente:

```
account required pam_faillock.so
```

Ahora nos toca probar si podemos cambiar nuestra contraseña con otro usuario, como en este sistema no puedo enseñar la contraseña que pongo por terminal os mostraré diversos errores que pueden salir:



Ahora tendré dos minutos de bloqueo de cuenta hasta poder volver a cambiar la contraseña, después de probar todos los requisitos puedo decir que funciona perfectamente.

3. Apartados Linux

Para empezar deberemos crear dos usuarios (alumnoFCT1/2) con sus directorios separados, deberán de tener su directorio de home como cualquier otro usuario y por ello poder iniciar sesión por GUI, estos usuarios estarán sujetos a las políticas de contraseñas establecidas anteriormente.

```
ubuntu@ubuntu-VirtualBox:~$ sudo adduser alumnoFCT1 --force-badname
ubuntu@ubuntu-VirtualBox:~$ sudo adduser alumnoFCT2 --force-badname
```

Ahora crearé un nuevo grupo (proyecto) y añadiré a ambos usuarios que acabos de crear, para comprobarlo usaré el comando id:

```
ubuntu@ubuntu-VirtualBox:~$ sudo groupadd proyecto
ubuntu@ubuntu-VirtualBox:~$ sudo usermod -G proyecto -a alumnoFCT1
ubuntu@ubuntu-VirtualBox:~$ sudo usermod -G proyecto -a alumnoFCT2
ubuntu@ubuntu-VirtualBox:~$ id alumnoFCT1
uid=1001(alumnoFCT1) gid=1001(alumnoFCT1)
grupos=1001(alumnoFCT1),1003(proyecto)
```

Ahora crearé el directorio proyectos y restringiré el acceso a todo el mundo que no pertenezca al grupo proyecto.

```
ubuntu@ubuntu-VirtualBox:~$ sudo mkdir /proyectos
ubuntu@ubuntu-VirtualBox:~$ sudo chown :proyecto /proyectos
ubuntu@ubuntu-VirtualBox:~$ sudo chmod 070 /proyectos
ubuntu@ubuntu-VirtualBox:~$ sudo ls -la /proyectos
total 8
d---rwx---  2 root proyecto 4096 oct 20 19:48 .
```

Para terminar limitaré el espacio de dicho directorio (proyecto), para ello primero instalare el paquete quote:

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt install quota
```

Para que las cuotas sean efectivas debemos de tener mas de un disco, para establecer el limite de quote escribiremos en el fstab lo siguiente:

```
ubuntu@ubuntu-VirtualBox:~$ sudo vim /etc/fstab
/dev/sdb /proyectos ext4 defaults,usrquota,grpquota 0 1
```

Ahora activaré las cuotas en el sistema (sdb):

```
ubuntu@ubuntu-VirtualBox:~$ sudo quotacheck -cum /proyectos
ubuntu@ubuntu-VirtualBox:~$ sudo quotaon -v /proyectos
```

Para finalizar pondremos el siguiente comando y limitaremos la quota del grupo proyecto por ejemplo a 250MB.

```
ubuntu@ubuntu-VirtualBox:~$ sudo edquota -g proyecto
Cuotas de disco para group proyecto (gid 1003):
  Sist. arch. bloques  blando       duro     inodos   blando     duro
  /dev/sdb1        0   200000      150000      0         0         0
```

```
Cuotas de disco para group proyecto (gid 1003):
  Sist. arch.                bloques     blando      duro     inodos   blando     duro
  /dev/sdb1                       0     200000     250000         0        0        0
```

Ahora podremos llenar la cuota de ficheros, después de hacerlo nos notificará como un mensaje y nos lo recordará cada vez que intentemos añadir o modificar información en ese directorio.

Problemas y soluciones

- En el apartado de Windows tarda un tiempo en cargar la nueva política.
- Para crear los usuarios he tenido que utilizar el parámetro --force-badname por un ajuste del sistema.

Bibliografía

- Web de referencia (https://aulavirtual3.educa.madrid.org/ies.alonsodeavellan.alcala/pluginfile.php/204271/mod_workshop/intro/Practica%201.10%20-%20Configuracion%20de%20contrase%C3%B1as%20en%20Windows%20y%20Linux%20y%20Gesti%C3%B3n%20de%20grupos.pdf?time=1731369393055)
- Windows políticas (https://www.infosecinstitute.com/resources/operating-system-security/how-to-configure-password-policies-in-windows-10/)
- Ubuntu políticas (https://askubuntu.com/questions/113682/how-to-change-disable-password-complexity-test-when-changing-password)

Conclusión:

Es una practica interesante al alterar diferentes políticas de contraseñas en ambos sistemas aunque, personalmente no veo el sentido al ultimo apartado de Linux.