Llistes de control d'accés (ACL)

Context:

Ets un administrador de sistemes en una petita empresa que gestiona fitxers crítics de diversos departaments. Necessites assegurar-te que els permisos sobre certs directoris i fitxers estiguin configurats correctament, atorgant o denegant accés segons sigui necessari. Per això utilitzaràs ACLs a Linux i Windows per donar un control més granular sobre els permisos.

Objectiu: Configurar ACLs per garantir que només certs usuaris i grups tinguin els permisos adequats sobre fitxers i directoris a Linux i Windows.

Part 1: Configuració d'ACL a Linux

Escenari

En un servidor Linux (Rocky p.ex.), tens una carpeta anomenada `/data/projectes` que conté fitxers de diferents projectes. Els empleats dels departaments de **Vendes** i **Desenvolupament** necessiten accedir als arxius de diferents maneres.

- Usuaris del departament de **Vendes** (vendes1, vendes2) necessiten tenir només permisos de lectura sobre el directori `/data/projectes`.
- Usuaris del departament de **Desenvolupament** (dev1, dev2) necessiten tenir permisos de lectura i escriptura.
- L'usuari **admin** ha de tenir tots els permisos (lectura, escriptura, execució).

Tasques

Configuració inicial

Verificació d'ACLs

Rocky Linux utilitza com a sistema d'arxius *XFS*, que soporta l'ús d'ACL per defecte. Encara i això, comproveu que es així fent ús del comandament: `cat /boot/config* | grep _ACL`

En la exidida del comandament anterior haurieu de vore algo paregut a:

```
CONFIG_EXT4_FS_POSIX_ACL=y
CONFIG_XFS_POSIX_ACL=y
```

- Crea la carpeta `/data/projectes`
- Fes que el propietari de la carpeta siga **root** i el grup **root**
- Els permisos bàsics inicials de la carpeta han de ser 770 (rwxrwx---)
- Crea en el sistema els usuaris que farem servir: *admin*, *vendes1*, *vendes2*, *dev1* i *dev2*
- A més, hauràs de crear un grup que es cride *devs* i ficar els usuaris *dev1* i *dev2* dins

Configuració de les ACL

Sobre la carpeta anterior, afegir ACL als usuaris del departament de Vendes:

- Els usuaris *vendes1* i *vendes2* han de tenir només permisos de escriptura

Afegeix ACL als usuaris del departament de Desenvolupament

- Els grup *devs* han de tenir permisos de lectura

Atorgar permisos complets a l'usuari admin:

- L'usuari *admin* ha de tenir tots els permisos (lectura, escriptura i execució)

Atenció

Recorda que sense les ACL per defecte, els fitxers creats no heretaran els permisos configurats.

Verificar les ACLs configurades amb el comandament i les captures de pantalla adequades.

Proves

- Crea un arxiu amb un dels usuaris de vendes i prova a llegir-lo. Pots fer-lo? Per què?
- Prova de llegir l'arxiu amb l'altre usuari de vendes. Pots fer-lo? Per què?
- Prova de modificar l'arxiu amb eixe segon usuari. Has tingut èxit? Per què?
- Prova de modificar l'arxiu amb un dels usuaris del grup *devs*

- Mostra el contingut del arxiu amb eixe usuari del grup *devs*
- Prova de crear un arxiu nou amb eixe usuari
- Verifiqueu que l'usuari **admin** tingui control total creant un nou arxiu, mostrant el contingut dels ja existents i modificant-los tots.

Part 2: Configuració d'ACLs a Windows

Escenari

En un servidor Windows, hi ha una carpeta anomenada `C:\Projectes` amb fitxers sensibles de l'empresa. Diferents usuaris necessiten diferents nivells d'accés.

Configuració inicial

- Crear la carpeta `C:\Projectes`
- Crear els usuaris *marketing1, marketing2, it1, it2* i *admin*
- Crea un grup amb el nom **it** i fica dins als usuaris *it1* i *it2*

Tasques

- Usuaris de l'equip de màrqueting (marketing1, marketing2) necessiten tenir permisos de només lectura sobre la carpeta.
- Usuaris de l'equip d'IT (it1, it2) necessiten tenir permisos de lectura i de escriptura.
- L'administrador (administrador) ha de tenir control total sobre la carpeta.

Verificar permisos de seguretat avançats

- Feu clic al botó Opcions avançades a la pestanya Seguretat per revisar els permisos heretats i les entrades ACL detallades.
- Assegureu-vos que els permisos aplicats als usuaris no s'heretin d'altres carpetes si no és necessari.

Proves:

- Verifica que els usuaris de Màrqueting no puguin modificar fitxers a C:\Projectes, però puguin llegir-los.
- Verifica que els usuaris de Màrqueting no puguin crear arxius o directoris.
- Verifica que els usuaris d'IT puguin llegir i modificar fitxers.

- Intenta crear amb un usuari del grup **it** un arxiu dins del directori amb el botó dret. Detalla què observes.
- Intenta crear amb un usuari del grup **it** un arxiu dins del directori des del mateix bloc de notes. Detalla què observes.
- Verifiqueu que l'administrador té control total sobre la carpeta.

Preguntes per a la reflexió

Pregunta 1

Quins avantatges ofereix la configuració d'ACL en comptes d'utilitzar només els permisos tradicionals (rwx a Linux o NTFS a Windows)?

Pregunta 2

Quins problemes podrien sorgir si un sistema no tingués suport per a ACL?

Pregunta 3

Com canviaria la configuració d'ACL si els permisos d'accés canviessin dinàmicament?