

# Acl sol

## Parte 1: Configuración de ACLs en Linux Soluciones técnicas:

Instalación y verificación de ACLs: Comando para instalar el soporte de ACLs (si no está instalado):

```
bash
```

```
sudo apt-get install acl
```

Verificación de que la partición tenga soporte ACL:

```
bash
```

```
mount | grep acl
```

Si no está habilitado, debes añadir la opción `acl` en el archivo `/etc/fstab` para la partición correspondiente y volver a montar la partición.

Configuración de permisos iniciales del directorio: Crear la carpeta y establecer permisos:

```
bash
```

```
sudo mkdir -p /data/proyectos sudo chown root:root /data/proyectos sudo chmod 770 /data/proyectos
```

ACLs para los usuarios del departamento de Ventas (solo lectura): Se asignan permisos de solo lectura a `ventas1` y `ventas2`:

```
bash
```

```
sudo setfacl -m u:ventas1:r /data/proyectos sudo setfacl -m u:ventas2:r /data/proyectos
```

ACLs para los usuarios del departamento de Desarrollo (lectura y escritura): Se otorgan permisos de lectura y escritura a `dev1` y `dev2`:

```
bash
```

```
sudo setfacl -m u:dev1:rw /data/proyectos sudo setfacl -m u:dev2:rw /data/proyectos
```

ACLs para el administrador (todos los permisos): El usuario `admin` recibe control total sobre el directorio:

```
bash
```

```
sudo setfacl -m u:admin:rwX /data/proyectos
```

Verificación de las ACLs configuradas: Para ver las ACLs actuales del directorio:

```
bash
```

```
getfacl /data/proyectos
```

Salida esperada:

text

```
# file: data/proyectos
# owner: root
# group: root
user::rwx
user:ventas1:r--
user:ventas2:r--
user:dev1:rw-
user:dev2:rw-
user:admin:rwx
group:---
mask::rwx
other:---
```

Pruebas:

Ventas (ventas1 y ventas2) deberían poder leer archivos en /data/proyectos pero no modificarlos.  
Desarrollo (dev1 y dev2) deberían poder leer y escribir archivos en /data/proyectos.  
Admin (admin) debería tener todos los permisos sobre los archivos y el directorio.

Parte 2: Configuración de ACLs en Windows Soluciones técnicas:

Crear la carpeta C:\Proyectos: Si la carpeta no existe, simplemente créala mediante el explorador de archivos o usando el comando:

```
cmd
```

```
mkdir C:\Proyectos
```

Permisos para los usuarios de Marketing (solo lectura): En la pestaña de Seguridad:

Selecciona Editar.

Añade marketing1 y marketing2.

Otorga permisos de solo lectura (Lectura y ejecución, Mostrar carpeta, Lectura).

Permisos para los usuarios de IT (lectura y modificación):

Añade it1 y it2.

Otórgales permisos de lectura y modificación (Lectura y ejecución, Mostrar

carpeta, Lectura, Modificar).

Control total para el Administrador:

Asegúrate de que el usuario Administrator tenga control total sobre la carpeta.

Verificación de permisos avanzados: Revisa las opciones avanzadas en la pestaña de Seguridad para confirmar que los permisos no sean heredados incorrectamente y que las ACLs sean correctas.

### Pruebas:

Marketing (marketing1 y marketing2) solo deben poder leer los archivos en C:\Proyectos, pero no modificarlos.

IT (it1 y it2) deben poder leer y modificar los archivos.

Administrador debe tener control total sobre la carpeta y su contenido.

### Preguntas para Reflexión:

¿Qué ventajas ofrece la configuración de ACLs en lugar de usar solo los permisos tradicionales (rwx en Linux o NTFS en Windows)?

Las ACLs ofrecen un control más granular sobre los permisos de archivos y directorios. En lugar de limitarse a los tres grupos (propietario, grupo, otros) en Linux o los permisos básicos en Windows, con ACLs puedes asignar permisos específicos a cualquier usuario o grupo, adaptando mejor los accesos a las necesidades reales de seguridad y operación.

ACLs permiten excepciones a las reglas generales de permisos, lo que es útil en situaciones complejas donde se requiere una mayor flexibilidad.

¿Qué problemas podrían surgir si un sistema no tuviera soporte para ACLs?

Sin ACLs, las empresas se ven limitadas a los permisos tradicionales, lo que puede ser insuficiente en entornos donde diferentes usuarios necesitan acceder a los mismos archivos con diferentes permisos. Esto podría llevar a riesgos de seguridad (demasiados permisos otorgados) o ineficiencia (la necesidad de crear muchas estructuras de directorios o usuarios adicionales).

También se complica la administración, ya que se pierde la capacidad de definir excepciones específicas para usuarios o grupos.

¿Cómo cambiaría la configuración de ACLs si los permisos de acceso cambiaran dinámicamente?

Si los permisos cambian frecuentemente, se debería considerar la creación de grupos dinámicos basados en roles, en lugar de gestionar cada usuario individualmente en las ACLs. Esto facilita el mantenimiento y permite un manejo más eficiente de los cambios.

Además, podría ser necesario implementar herramientas automatizadas o políticas que ajusten dinámicamente las ACLs según las necesidades de acceso (por ejemplo, scripts de automatización o herramientas de gestión centralizada como Active Directory en Windows o Ansible en Linux).

Este ejercicio completo, con soluciones, cubre tanto la parte técnica como la reflexión teórica, permitiendo que tus estudiantes aprendan los fundamentos y las ventajas del uso de ACLs en sistemas operativos comunes.