

2.9.- Creación de políticas de autorización.

La etiqueta **<Limit>** en ProFTPD es una herramienta esencial para controlar el acceso y las acciones que los usuarios pueden realizar en tu servidor FTP. Se utiliza para aplicar restricciones sobre una amplia gama de operaciones FTP, permitiendo a los administradores del servidor definir políticas de seguridad detalladas y adaptadas a sus necesidades específicas. Dentro de un bloque **<Limit>**, puedes especificar varias operaciones FTP para restringir, tales como:

- ✓ **READ**: Limita operaciones de lectura como RETR (descargar archivos).
- ✓ **WRITE**: Restringe operaciones de escritura como STOR (subir archivos), STOU, APPE.
- ✓ **DIRS**: Afecta comandos que listan directorios o cambian directorios, como LIST, NLST, CWD, CDUP.
- ✓ **DELETE**: Restringe la eliminación de archivos y directorios con DELE, RMD.
- ✓ **RENAME**: Controla el cambio de nombre de archivos y directorios con RNFR, RNT0.
- ✓ **ALL**: Aplica restricciones a todas las operaciones FTP disponibles.

Uso de Directivas **Allow**, **Deny** y **Order**

Las directivas **Allow** y **Deny** se utilizan dentro de un bloque **<Limit>** para especificar quién tiene permitido o denegado realizar las operaciones restringidas. La directiva **Order** determina el orden en que se evalúan estas reglas.

Ejemplo Completo

Supongamos que quieres configurar un servidor FTP con las siguientes políticas:

- Todos los usuarios pueden leer archivos (READ), pero solo ciertos usuarios pueden subir o modificar archivos (WRITE).
- Solo un grupo específico puede eliminar archivos (DELETE).
- Nadie puede renombrar archivos (RENAME), excepto el administrador.

La configuración en proftpd.conf podría verse así:

```
<VirtualHost ftp.example.com>
  ServerName "Mi Servidor FTP"

  # Permitir a todos leer archivos
  <Limit READ>
    AllowAll
  </Limit>

  # Restringir escritura solo a usuarios específicos
  <Limit WRITE>
    Order Deny,Allow
    DenyAll
    AllowUser user1 user2
  </Limit>

  # Solo permitir eliminar archivos a miembros del grupo 'editores'
  <Limit DELETE>
    Order Allow,Deny
    AllowGroup editores
    DenyAll
  </Limit>

  # Restringir el cambio de nombre, excepto para el administrador
```

```
<Limit RENAME>
  Order Deny,Allow
  DenyAll
  AllowUser admin
</Limit>
</VirtualHost>
```

- **<Limit READ>**: Esta sección permite a todos los usuarios realizar operaciones de lectura. No se necesita Order porque AllowAll es la única regla.
- **<Limit WRITE>**: Aquí se utiliza Order Deny,Allow para primero bloquear a todos (DenyAll) y luego permitir explícitamente a user1 y user2. Esto significa que, por defecto, nadie puede escribir, excepto estos dos usuarios.
- **<Limit DELETE>**: Se configura con Order Allow,Deny, lo que significa que primero se procesan las directivas Allow. En este caso, los miembros del grupo editores pueden eliminar archivos, y luego DenyAll bloquea esta acción a cualquier otro usuario que no sea miembro del grupo.
- **<Limit RENAME>**: Similar a WRITE, se niega la acción a todos excepto al usuario admin, que tiene permiso explícito para renombrar archivos.

Lha directiva **Order** es crucial porque define cómo se aplican las reglas **Allow** y **Deny**. **Allow,Deny** significa que si un usuario pasa una regla **Allow**, se le permitirá la acción a menos que una regla **Deny** también se aplique. **Deny,Allow** significa que se aplican todas las restricciones hasta que una regla Allow específicamente concede acceso.

Estas configuraciones permiten crear un entorno FTP más seguro y controlado, donde solo usuarios y grupos específicos tienen permisos para realizar ciertas acciones, limitando la posibilidad de acciones no autorizadas.



Debes conocer

En el siguiente enlace encontrarás información sobre la directiva Order de ProFTPD.

[Directiva Order de ProFTPD.](#)

En el siguiente enlace encontrarás información sobre la directiva Allow de ProFTPD.

[Directiva Allow de ProFTPD.](#)

En el siguiente enlace encontrarás información sobre la directiva Deny de ProFTPD.

[Directiva Deny de ProFTPD.](#)