PAM es un mecanismo de autenticación flexible que permite abstraer a las aplicaciones y otro software del proceso de identificación. Su implementación se realiza mediante una biblioteca de enlace dinámico.

Para averiguar si un programa utiliza PAM, se puede usar el comando ldd.

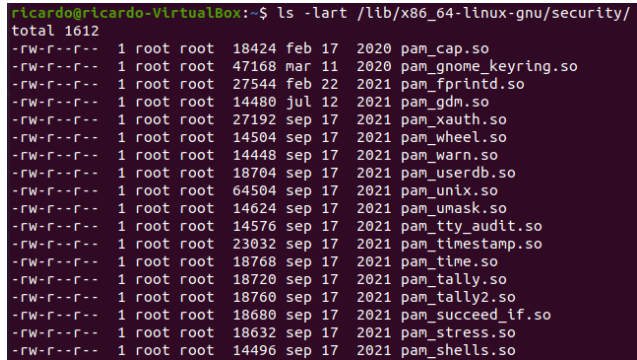


**Biblioteca principal**:

* /lib/x86\_64-linux-gnu/libpam.so.0

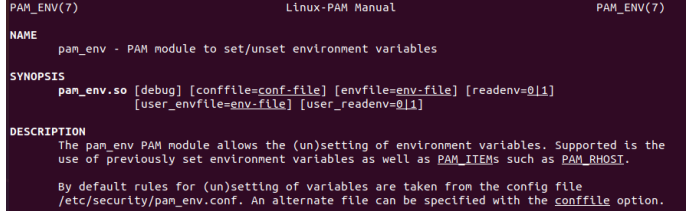
**Módulos conectables**:

* Ubicados en /lib/x86\_64-linux-gnu/security
* Ejemplos: pam\_unix.so, pam\_ldap.so, pam\_winbind.so

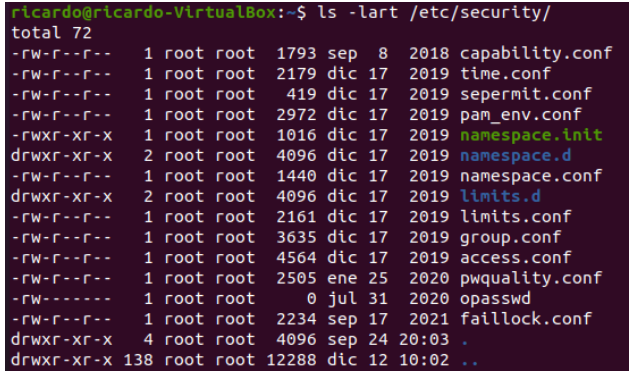


La utilidad y configuración de cada módulo están documentadas en el manual del sistema. Ejemplos:

* man pam\_unix
* man pam\_ldap

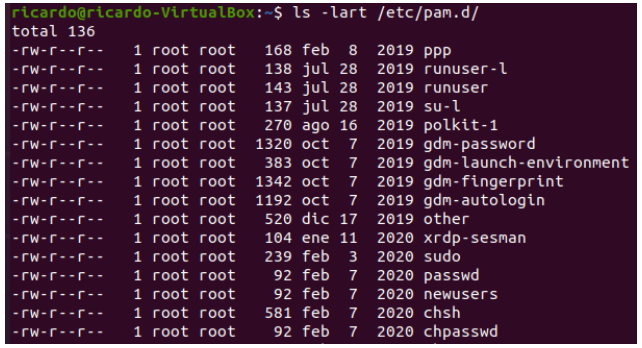


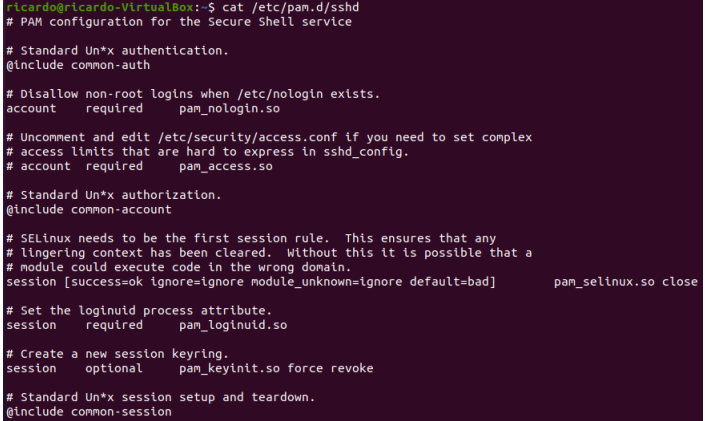
* **Parámetros de configuración**: La mayoría de los módulos se configuran mediante parámetros pasados en el momento de su invocación.
* **Ficheros de configuración**: Algunos módulos especiales tienen ficheros de configuración dedicados en /etc/security.  
  + Módulo: pam\_limits
  + Fichero: /etc/security/pam\_limits.conf



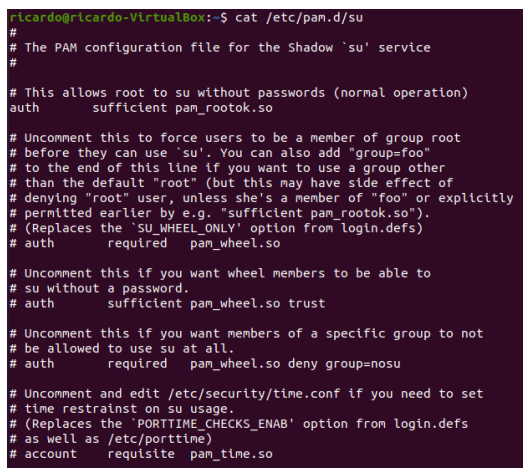
1. **Fichero por defecto**: /etc/pam.conf  
   Define los módulos PAM utilizados por los programas que emplean PAM, como login, sshd, gdm, y passwd.
2. **Configuración en directorios**:  
   En instalaciones actuales, el directorio /etc/pam.d reemplaza al fichero /etc/pam.conf. Contiene un fichero de configuración para cada programa que use PAM:
   * /etc/pam.d/login
   * /etc/pam.d/sshd
   * /etc/pam.d/lightdm
   * /etc/pam.d/passwd
3. **Fichero genérico**:  
   /etc/pam.d/other se utiliza para configurar programas que emplean PAM pero no disponen de un fichero propio.







El archivo suele contener una serie de directivas que especifican los módulos PAM y cómo deben ser utilizados



#### **Comportamiento del archivo**

1. **Restricción a miembros del grupo wheel**Si la línea pam\_wheel.so está activa, solo los usuarios pertenecientes al grupo wheel podrán utilizar el comando su. Esto mejora la seguridad al restringir quién puede cambiar de usuario.
2. **Compatibilidad con otros módulos**La inclusión de reglas comunes a través de system-auth permite compartir los mismos mecanismos de autenticación entre diferentes servicios del sistema.
3. **Modularidad**PAM facilita la personalización del comportamiento del comando su mediante la adición o modificación de módulos

#### **Comportamiento si el archivo no existe**

1. El comando su **podría no funcionar**, ya que PAM no tendría reglas definidas para manejar la autenticación de este servicio.
2. Dependiendo de la configuración del sistema, **se generará un error** indicando que el archivo de configuración no se encuentra

### **¿Qué hace cada módulo?**

* **pam\_rootok.so**: Permite a root ejecutar su sin contraseña.
* **pam\_wheel.so**: Controla el acceso al comando su basado en la pertenencia a grupos.
* **pam\_time.so**: Permite configurar restricciones temporales para el uso de su.