Pluggable Authentication Modules(PAM)

Ampliación de Sistemas Operativos

Yeray Valdivia López

¿Qué es PAM?

- Los programas que permiten a los usuarios accesar un sistema deben verificar la identidad del usuario a través de un proceso que se denomina AUTENTIFICAR.
- PAM es un mecanismo flexible para la autenticación de usuarios.
- PAM utiliza una arquitectura conectable y modular, que otorga al administrador del sistema de una gran flexibilidad en establecer las políticas de autenticación para el sistema.
- PAM permite el desarrollo de programas independientes del mecanismo de autenticación a utilizar.

Ventajas que ofrece PAM

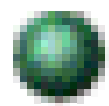
- Ofrece un esquema de autenticación común y centralizado.
- Permite a los desarrolladores abstraerse de las labores de autenticación.
- Facilita el mantenimiento de las aplicaciones.
- Ofrece flexibilidad y control tanto al desarrollador como al administrador del sistema.

Grupos de gestión

- PAM no solo se encarga de verificar que un usuario sea quien dice ser.
- Existen 4 áreas de gestión, cada una de los cuales se encarga de un aspecto diferente de los servicios restringidos.

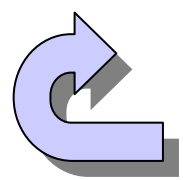
Grupos de gestión

- Account
- Auth
- Password
- Session

Continuar 

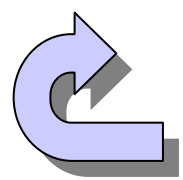
Account (cuenta)

- Servicios de verificación de cuentas de usuario.
- Ejemplos:
  - Permitir/denegar acceso en función de la hora
  - De los recursos disponibles
  - Si la cuenta ha caducado
  - ...



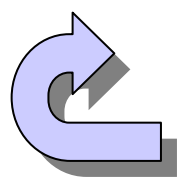
Auth (autenticación)

- Comprueba la identidad de los usuarios.
- Ofrecen un sistema de credenciales que permiten al usuario ganar ciertos privilegios (fijados por el administrador).



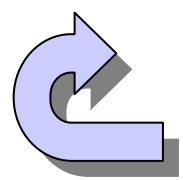
Password (contraseña)

- Se encarga de mantener actualizado el elemento de autenticación asociado a cada usuario (contraseña).



Session (sesión)

- Estos módulos configuran y administran sesiones de usuarios.
- Los módulos con esta interfaz también pueden realizar tareas adicionales que son necesitadas para permitir acceso, como el montaje de directorios principales de usuarios y hacer el buzón de correo disponible.



Comunicación con PAM

- Una aplicación X quiere hacer uso de las facilidades ofrecidas por PAM.
- Interactúa con la biblioteca de Linux-PAM, sin tener ningún detalle de cómo está configurado el sistema para la aplicación X.
- La biblioteca lee la configuración de PAM para saber qué política de autenticación ha de aplicarse.
- Para ello han de combinarse convenientemente los módulos.

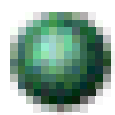
Configuración

- Existen dos esquemas diferentes:
  - La más antigua coloca toda la configuración en “etc/pam.conf”
  - Colocar la configuración de cada servicio en el directorio “etc/pam.d/
- Red Hat utiliza una combinación de ambas.

Reglas

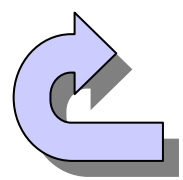
- Componen los ficheros de configuración de PAM

servicio*	tipo	control	ruta	[argumentos]

Continuar 

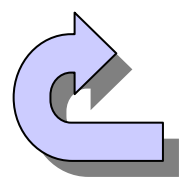
Servicio

- Indica el nombre de la aplicación/servicio correspondiente.
- Se utiliza sólo en /etc/pam.conf
- Existe un nombre de servicio reservado (“other”), que se utiliza para especificar las reglas por defecto.



Tipo

- Área de gestión a la que se destina la regla.
  - Auth
  - Account
  - Session
  - password

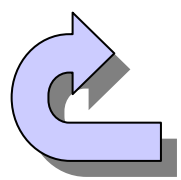


Control

- Indica a PAM que hacer en caso de éxito o fallo del módulo de la regla en cuestión.
- El orden de la pila de módulos hay que tenerlo mucho en cuenta para que actúe como se espera.
- Existen dos sintaxis:
  - Palabra clave única
  - Pares [valor-acción]

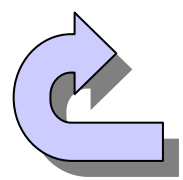
Sintaxis sencilla

- Required
- Requisite
- Sufficient
- Optional



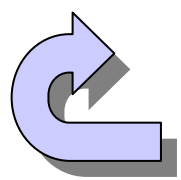
Required

- Indica que es necesario que el módulo tenga éxito para que la pila también lo tenga. Si se produce un fallo, no se notifica hasta que se procesa el resto de la pila.



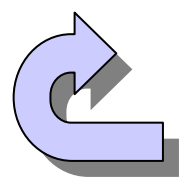
Requisite

- En esencia, es igual que el anterior, con la diferencia de que en caso de fallo, el control se devuelve inmediatamente a la aplicación.



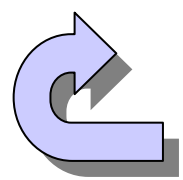
Sufficient

- El éxito en este módulo, si no se ha producido un fallo en los procesados anteriormente en la pila, es “suficiente”. Llegados a este punto, el procesamiento se detiene —ignorando incluso posibles required posteriores—. Un fallo no siempre resulta definitivo para la pila.



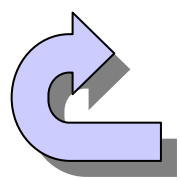
Optional

- Por lo general, PAM ignora los módulos marcados con este indicador. Su valor será tenido en cuenta sólo en caso de que no se haya llegado a ningún valor concreto de éxito o fracaso



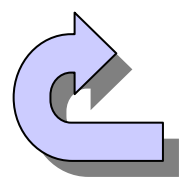
Ruta

- Este campo contiene la ruta del módulo que se va a utilizar: si empieza por el carácter ‘/’ se indica una ruta absoluta. En otro caso, será relativa a “/lib/security/”.



Argumentos

- Se trata de argumentos que pueden ser pasados al módulo para su operación.
- Generalmente, los argumentos son específicos para cada módulo y deberían estar documentados.
- Si se pasara un argumento no válido, el módulo lo ignoraría, aunque debería usar syslog para informar del error.

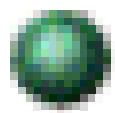


Algunos módulos

- Esta sección está dedicada a describir, sin entrar en demasiado detalle, algunos de los módulos que ofrece PAM.
- Los módulos se encuentran en “/lib/security/”.

Módulos

- Pam_cracklib.so
- Pam_deny.so
- Pam_env.so
- Pam_limits.so
- Pam_stack.so
- Pam_console.so
- Pam_nologin.so
- Pam_permit.so
- Pam_rootok.so
- Pam_securety.so
- Pam_wheel.so
- Pam_xauth.so

Continuar 

Pam_cracklib.so (password)

- Este módulo entra en funcionamiento cuando se establece o modifica la clave de un usuario.
- Si la clave no se “rompe” usando un diccionario, se la somete a una serie de comprobaciones.
- Posee un conjunto de argumentos.

Pam_cracklib.so (password) Comprobaciones

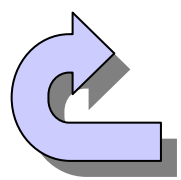
- Palíndromo: comprueba que la clave no sea la vieja pero al revés.
- Cambio de mayúsculas: realiza varias combinaciones cambiando mayúsculas por minúsculas y viceversa.
- Similar: comprueba que las claves se diferencian en **difok** caracteres.
- Simple: verifica el tamaño de la clave.
- Rotada: comprueba que no sea una rotación de la antigua.
- Ya usada: asegura que la clave no ha sido usada anteriormente (/etc/security/opasswd/)

Pam_cracklib.so (password) Argumentos

- Debug: muestra información detallada a través de syslog.
- Retry=N,(1): Especifica el número de veces que se pedirá la clave en caso de que no sea segura.
- Difok=N,(1/2 clave): Indica el número de caracteres que tienen que cambiar en la nueva clave.
- Minlen=N,(6): Indica el número mínimo de caracteres que tiene que tener la clave.
- Use_authok: Toma como nueva contraseña la obtenida por el módulo anterior.

Pam_cracklib.so (password) Argumentos

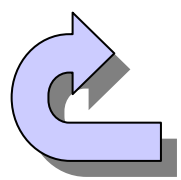
- dcredit=N,(1): Indica el máximo crédito para a los dígitos en las nuevas contraseñas.
- ucredit=N,(1): Indica el máximo crédito para dar a las mayúsculas en las nuevas contraseñas.
- lcredit=N,(1):Indica el máximo crédito para dar a las minúsculas en las nuevas contraseñas.
- ocredit=N,(1): Indica el máximo crédito para dar a otros caracteres en las nuevas contraseñas.



Pam_deny.so

(account, auth, password y session)

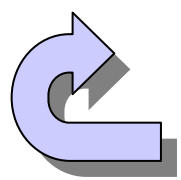
- El objetivo de éste módulo es producir un fallo siempre.



Pam_env.so (auth)

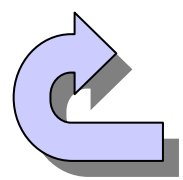
- Permite establecer las variables de entorno por defecto o sustituir los valores de las variables ya establecidas cuando un usuario se registra en el sistema. El fichero donde se definen dichas variables se encuentra en
  “/etc/security/pam env.conf”
- Las cláusulas de este fichero son de la siguiente manera:

VARIABLE [DEFAULT=[valor]] [OVERRIDE=[valor]]



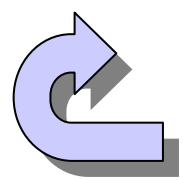
Pam_env.so (auth) Argumentos

- Debug
- conffile=fichero: Especifica el fichero de configuración alternativo.
- envfile=fichero: Especifica el fichero alternativo a “/etc/enviroment” que contiene las variables de entorno establecidas para el sistema.
- readenv=0/1: Especifica si se lee o no el fichero con las variables de entorno. Por defecto sí se lee.



Pam_limits.so (session)

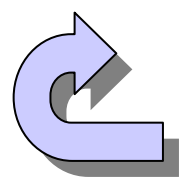
- Controla los límites impuestos en el fichero “/etc/security/limits.conf” a los recursos disponibles. Las limitaciones se pueden aplicar a un usuario, a un grupo o a todos los usuarios del sistema.



Pam_stack.so

(account, auth, password y session)

- Este módulo permite la asociación en pila de varios módulos PAM devolviendo un acierto, en caso de que toda la pila devuelva un acierto.
- En caso de que uno de los módulos de la pila devuelva un error, pam_stack devolverá el código de error devuelto por el módulo que ha fallado.



Ejemplos de configuración

- System-auth
- Passwd
- Other

Referencias

- Manual de referencia de Red Hat Linux 9
- Exposición de PAM (ASO 2003)
- Manual de PAM

FIN