Curso avanzado de Linux

Rafael Varela Pet

Unidad de Sistemas
Área de Tecnologías de la Información y Comunicaciones
Universidad de Santiago de Compostela

Curso avanzado de Linux

Autentificación. PAM.

PAM

- PAM: *Pluggable Authentication Modules*
- Conjunto de librerías compartidas que permiten a las aplicaciones solicitar que un usuario se autentifique
- “De serie” en cualquier distribución Linux moderna
- El administrador puede elegir cómo desea que las aplicaciones autentiquen a los usuarios

PAM

- 4 tareas de gestión:
  - autentificación: se establece que el usuario es quién dice ser.
  - account: gestión de tareas no asociadas a la autentificación (restricciones de acceso en función de la hora, carga del sistema, etc.).
  - sesión: tareas a ejecutar antes o después de que se le conceda al usuario el acceso a un determinado servicio
  - password: gestión del cambio del testigo del usuario

PAM

- Configuración en /etc/pam.conf o /etc/pam.d/ (Preferiblemente en /etc/pam.d)
- Librerías en /lib/security
- Formato de los ficheros en pam.d:

  tipo control camino_modulo parametros_modulo

  ...
- Tipo. Se corresponde con las 4 tareas:
  - auth - session
  - account - password

PAM - Control

- Bandera de control: determina como se va a reaccionar ante el fallo o éxito del módulo.
- Tipos:
  - *required*; indica que es necesario que este módulo tenga éxito, pero el fallo no será visible por el usuario hasta que se ejecuten los restantes módulos
  - requisite: igual que *required*, pero en este caso, si se produce un fallo, el control se devuelve inmediatamente.

PAM - Control

- Tipos (cont):
  - *sufficient*: Si ningún módulo anterior requerido ha fallado, no se llama a ningún módulo más.
  - *optional*: En general este módulo será ignorado, salvo que no haya una respuesta definitiva en el resto de los módulos.
  - *include*: incluye el contenido de otro fichero de configuración

PAM – Aplicaciones no configuradas

- Configuración aplicada a las aplicaciones que no tienen su propio fichero

  /etc/pam.d/other

- Asegurar configuración:

```
auth        required    pam_deny.so
auth        required    pam_warn.so
account     required    pam_deny.so
account     required    pam_warn.so

password    required    pam_deny.so
password    required    pam_warn.so
session     required    pam_deny.so
session     required    pam_warn.so
```

PAM – Ejemplos

- /bin/login
  - Debe validar que un usuario es quien dice ser
  - Si la autenticación es correcta, entrega un servicio (una shell)
- Configuración en /etc/pam.d/login
- Autentificación clásica UNIX:

  ```
  auth required pam_unix.so nullok_secure
  ```
- Permitir la entrada sin contraseña. :

  ```
  auth sufficient pam_permit.so
  ```

PAM - Ejemplos

- Incorporar un nuevo mecanismo de autenticación
- Ejemplo con usuarios en base de datos tipo Berkeley DB (.db) versión 4.3:
  - Instalar utilidades para Berkeley DB:
    aptitude install db4.3_load
  - Crear fichero .db:
    db4.3_load -T -t hash usuarios.db < usuarios.txt
  - Editar /etc/pam.d/login:
    auth sufficient pam_userdb.so db=/tmp/usuarios

PAM - libpam-ssh

- Permite disponer de 'single sign-on' en nuestras conexiones SSH cuando empleamos autenticación de clave pública
- Podemos desbloquear automáticamente nuestra identidad SSH
- Si queremos hacerlo al iniciar sesión en GNOME empleando GDM:
  - aptitude install libpam-ssh
  - editar el fichero /etc/pam.d/gdm

PAM - libpam-ssh

- Fichero /etc/pam.d/gdm:

```
auth     requisite      pam_nologin.so
auth     required       pam_env.so
@include common-auth
@include pam-ssh-auth
@include common-account
session  required       pam_limits.so
@include common-session
@include pam-ssh-session
@include common-password
```

PAM - libpam-ssh

- También podemos autenticamos con la clave de nuestra identidad SSH:

```
auth     requisite      pam_nologin.so
auth     required       pam_env.so
@include pam-ssh-auth
@include common-auth
@include common-account
session  required       pam_limits.so
@include common-session
@include pam-ssh-session
@include common-password
```

PAM - libpam-mount

- Monta un sistema de archivos para la sesión de un usuario
- Editar fichero correspondiente en /etc/pam.d, añadiendo al final:

  ```
  @include common-pammount
  ```

- Posibilidades:
  - smbfs: monta recursos compartidos windows
  - sshfs, loopback
  - en general, cualquier sistema de archivos que el kernel sea capaz de usar

PAM - libpam-mount

- Debemos ajustar el fichero /etc/security/pam_mount.conf
- Ejemplos:
  - Montar dispositivos loopback:

```
volume @@users auto -
    /home/&.img /mnt/&
    loop,user,exec - -
```

  - Montar un sistema de archivos remoto sobre SSH:

```
volume @@users fuse -
"sshfs#&@aula00:" /mnt/& - - -
```

Referencias

- libpam-doc: file:///usr/share/doc/libpam-doc/html/pam.html