Autenticación PAM - Redes PYMES

Índice general de la serie: Redes de Computadoras para las PYMES: Introducción

Autor: Federico A. Valdes Toujague
federicotoujague@gmail.com
http://blog.desdelinux.net/author/fico

¡Hola amigas y amigos!

Con este artículo pretendemos ofrecer una Visión General al tema de la Autenticación mediante PAM. Estamos acostumbrados a utilizar diariamente nuestra Estación de Trabajo con algún sistema operativo Linux/UNIX y en pocas ocasiones nos detenemos a estudiar el cómo se produce el mecanismo de autenticación cada vez que iniciamos una sesión. Acaso conocemos de la existencia de los archivos ***/etc/passwd***, y ***/etc/shadow*** que constituyen la base de datos principal de las Credenciales de Autenticación de los usuarios locales. Esperamos que después de la lectura de este post se disponga -al menos- de una idea clara de cómo funciona PAM.

Autenticación

La Autenticación -para propósitos prácticos- es la forma en que un usuario se verifica ante un sistema. El proceso de autenticación requiere la presencia de un juego de identidad y credenciales -nombre de usuario y su contraseña- las que se comparan con la información almacenada en alguna base de datos. Si las credenciales presentadas son iguales a las almacenadas y la cuenta del usuario está activa, se dice que el usuario se **autenticó** correctamente o que pasó satisfactoriamente el proceso de **autenticación**.

Una vez que el usuario se autenticó, se pasa esa información al **servicio de control de acceso** para determinar qué puede hacer ese usuario en el sistema y a cuales recursos tiene la debida **autorización** para acceder a ellos.

La información para verificar al usuario pueden almacenarse en bases de datos locales del sistema, o el sistema local puede hacer referencia a una base de datos existente en un sistema remoto, tales como bases de datos LDAP, Kerberos, NIS, etcétera.

La mayoría de los sistemas operativos UNIX®/Linux tienen las herramientas necesarias para configurar el servicio de autenticación cliente/servidor de los tipos mas comunes de base de datos de usuarios. Algunas de esos sistemas disponen de herramientas gráficas muy completas como Red Hat / CentOS, SUSE / openSUSE, y otras distribuciones.

PAM: Pluggable Authentication Module

Los **Módulos que se Insertan para la Autenticación** los utilizamos diariamente cuando iniciamos sesión en nuestro Desktop con un sistema operativo basado en Linux/UNIX, y en muchas otras ocasiones que accedemos a servicios locales o remotos que tienen un determinado módulo local PAM *insertado* para la autenticación frente a ese servicio.

Una idea práctica de como se Insertan los Módulos PAM la podemos obtener mediante la secuencia del estado de la autenticación en un

equipo con Debian y en otro con CentOS que desarrollamos a continuación.

Debian

Documentación

Si instalamos el paquete ***libpam-doc*** dispondremos de una muy buena documentación ubicada en el directorio */usr/share/doc/libpam-doc/html*.

```
root@linuxbox:~# aptitude install libpam-doc
root@linuxbox:~# ls -l /usr/share/doc/libpam-doc/
```

También existe más documentación sobre PAM en los directorios:

```
root@linuxbox:~# ls -l /usr/share/doc/ | grep pam
drwxr-xr-x  2 root root 4096 abr  5 21:11 libpam0g
drwxr-xr-x  4 root root 4096 abr  7 16:31 libpam-doc
drwxr-xr-x  2 root root 4096 abr  5 21:30 libpam-gnome-keyring
drwxr-xr-x  3 root root 4096 abr  5 21:11 libpam-modules
drwxr-xr-x  2 root root 4096 abr  5 21:11 libpam-modules-bin
drwxr-xr-x  2 root root 4096 abr  5 21:11 libpam-runtime
drwxr-xr-x  2 root root 4096 abr  5 21:26 libpam-systemd
drwxr-xr-x  3 root root 4096 abr  5 21:31 python-pam
```

Opinamos que antes de salir a buscar documentación en la Internet, debemos revisar la que ya está instalada o la que podemos instalar directamente de los repositorios de programas que para algo existen y en muchas ocasiones los copiamos hacia nuestro disco duro. Muestra de ello es la siguiente:

```
root@linuxbox:~# less /usr/share/doc/libpam-gnome-keyring/README
gnome-keyring is a program that keep password and other secrets for
users. It is run as a daemon in the session, similar to ssh-agent, and
other applications locate it via an environment variable or a D-Bus.

The program can manage several keyrings, each with its own master
password, and there is also a session keyring which is never stored to
disk, but forgotten when the session ends.

The library libgnome-keyring is used by applications to integrate with
the GNOME keyring system.
```

Que traducido muy libremente quiere expresar:

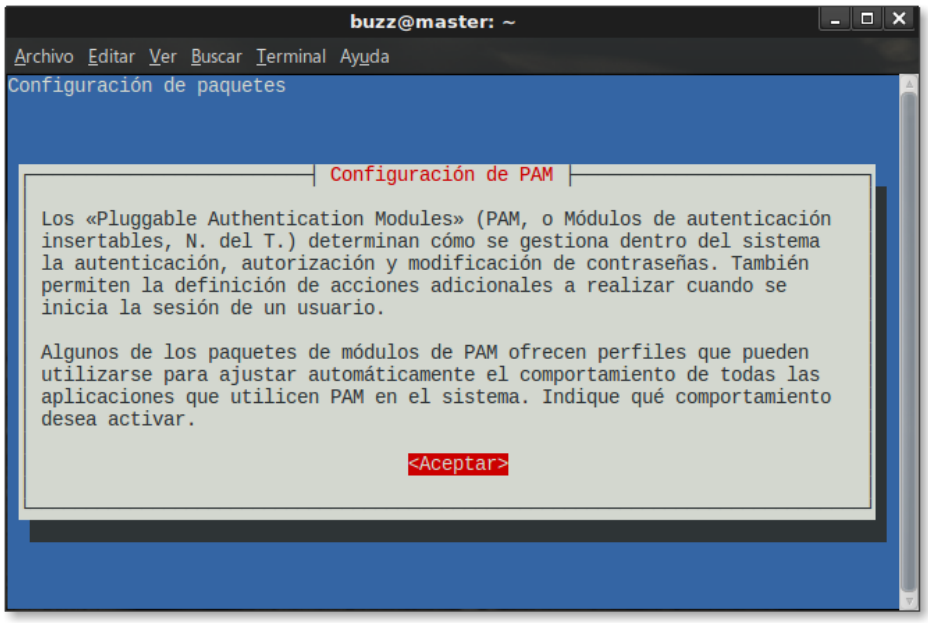
- *gnome-keyring es el programa encargado de mantener las contraseñas y otros secretos para los usuarios. En cada sesión se ejecuta como un demonio, de forma similar al ssh-agent, y a otras aplicaciones que se localizan mediante una variable del ambiente - environment o vía D-Bus. El programa puede manejar a varios keyrings, cada uno de ellos con su propia contraseña maestra. Existe además una sesión del keyring que no se almacena nunca en el disco duro y que se olvida cuando termina la sesión. Las Aplicaciones utilizan la librería libgnome-keyring para integrarse con el sistema GNOME keyring.*

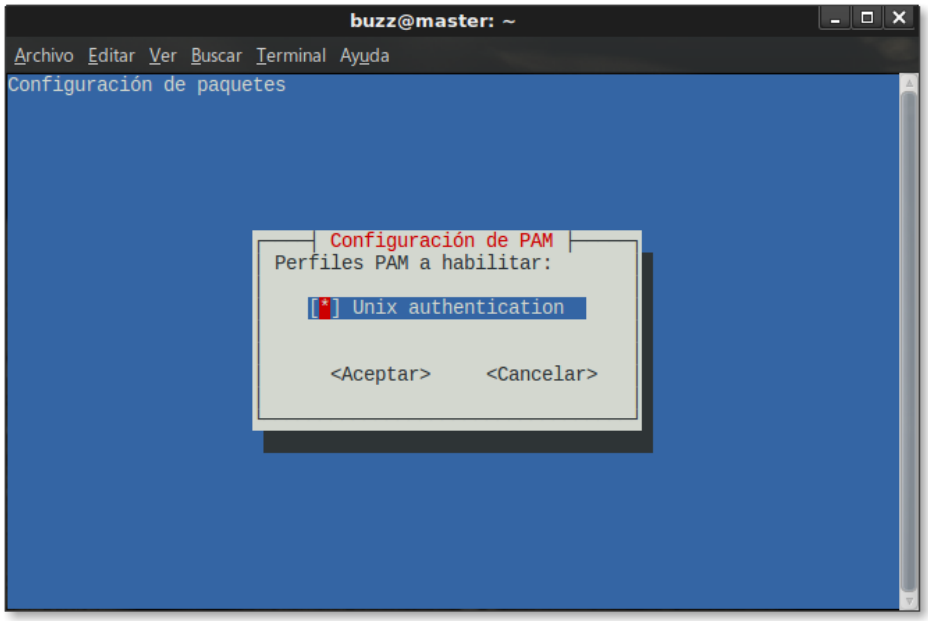
Debian con el Sistema Operativo Base

Partimos de un equipo al que recién instalamos Debian 8 "Jessie" como Sistema Operativo y durante su proceso de instalación seleccionamos solamente las "Utilidades básicas del sistema", sin marcar ninguna otra opción de instalar tareas - *tasks* o paquetes predefinidos como el servidor OpenSSH. Si después de iniciar la primera sesión ejecutamos:

```
root@master:~# pam-auth-update
```

obtendremos las siguientes salidas:





Lo que nos muestra que el único Módulo PAM en uso hasta ese momento es la Autenticación UNIX. La utilidad ***pam-auth-update*** nos permite configurar la política central de autenticación para un sistema al utilizar Perfiles Predefinidos que suministran los Módulos PAM. Para mas información consulte *man pam-auth-update*.

Como aun no hemos instalado el OpenSSH server, no encontraremos su módulo PAM en el directorio */etc/pam.d/*, el que contendrá los módulos y perfiles PAM cargados hasta éstos momentos:

```
root@master:~# ls -l /etc/pam.d/
total 76
-rw-r--r-- 1 root root  235 sep 30  2014 atd
-rw-r--r-- 1 root root 1208 abr  6 22:06 common-account
-rw-r--r-- 1 root root 1221 abr  6 22:06 common-auth
-rw-r--r-- 1 root root 1440 abr  6 22:06 common-password
-rw-r--r-- 1 root root 1156 abr  6 22:06 common-session
-rw-r--r-- 1 root root 1154 abr  6 22:06 common-session-noninteractive
-rw-r--r-- 1 root root  606 jun 11  2015 cron
-rw-r--r-- 1 root root  384 nov 19  2014 chfn
```

```
-rw-r--r-- 1 root root   92 nov 19  2014 chpasswd
-rw-r--r-- 1 root root  581 nov 19  2014 chsh
-rw-r--r-- 1 root root 4756 nov 19  2014 login
-rw-r--r-- 1 root root   92 nov 19  2014 newusers
-rw-r--r-- 1 root root  520 ene  6  2016 other
-rw-r--r-- 1 root root   92 nov 19  2014 passwd
-rw-r--r-- 1 root root  143 mar 29  2015 runuser
-rw-r--r-- 1 root root  138 mar 29  2015 runuser-l
-rw-r--r-- 1 root root 2257 nov 19  2014 su
-rw-r--r-- 1 root root  220 sep  2  2016 systemd-user
```

Por ejemplo, mediante el módulo PAM */etc/pam.d/chfn* el sistema configura el servicio *Shadow*, mientras que mediante */etc/pam.d/cron* se configura el demonio *cron*. Para conocer un poco mas podemos leer el contenido de cada uno de éstos archivos lo cual es muy instructivo. Como muestra damos a continuación el contenido del módulo */etc/pam.d/cron*:

```
root@master:~# less /etc/pam.d/cron
# The PAM configuration file for the cron daemon

@include common-auth

# Sets the loginuid process attribute
session    required     pam_loginuid.so

# Read environment variables from pam_env's default files, /etc/environment
# and /etc/security/pam_env.conf.
session       required   pam_env.so

# In addition, read system locale information
session       required   pam_env.so envfile=/etc/default/locale

@include common-account
@include common-session-noninteractive

# Sets up user limits, please define limits for cron tasks
# through /etc/security/limits.conf
session    required   pam_limits.so
```

El orden de las declaraciones dentro de cada uno de los archivos es importante. En términos generales no recomendamos se modifiquen ninguno de ellos a menos que sepamos muy bien qué es lo que estamos haciendo.

Debian con sistema operativo base + OpenSSH

```
root@master:~# aptitude install task-ssh-server
Se instalarán los siguiente paquetes NUEVOS:
  openssh-server{a} openssh-sftp-server{a} task-ssh-server
```

Comprobaremos que se agregó y configuró correctamente el módulo PAM *sshd*:

```
root@master:~# ls -l /etc/pam.d/sshd
-rw-r--r-- 1 root root 2133 jul 22  2016 /etc/pam.d/sshd
```

Si deseamos conocer el contenido de ese perfil:

```
root@master:~# less /etc/pam.d/sshd
```

En otras palabras, cuando tratamos de iniciar una sesión remota desde otro equipo mediante *ssh*, la autenticación en el equipo local se efectúa mediante el módulo PAM *sshd* principalmente, sin olvidar los demás aspectos de autorización y seguridad involucrados en el servicio ssh como tal.

De paso, añadimos que el archivo principal de configuración de este servicio es */etc/ssh/sshd_config*, y que al menos en Debian se instala por defecto sin permitir el inicio de sesión interactivo del usuario *root*. Para permitirlo, debemos modificar el archivo */etc/ssh/sshd_config* y cambiar la línea:

```
PermitRootLogin without-password
```

por

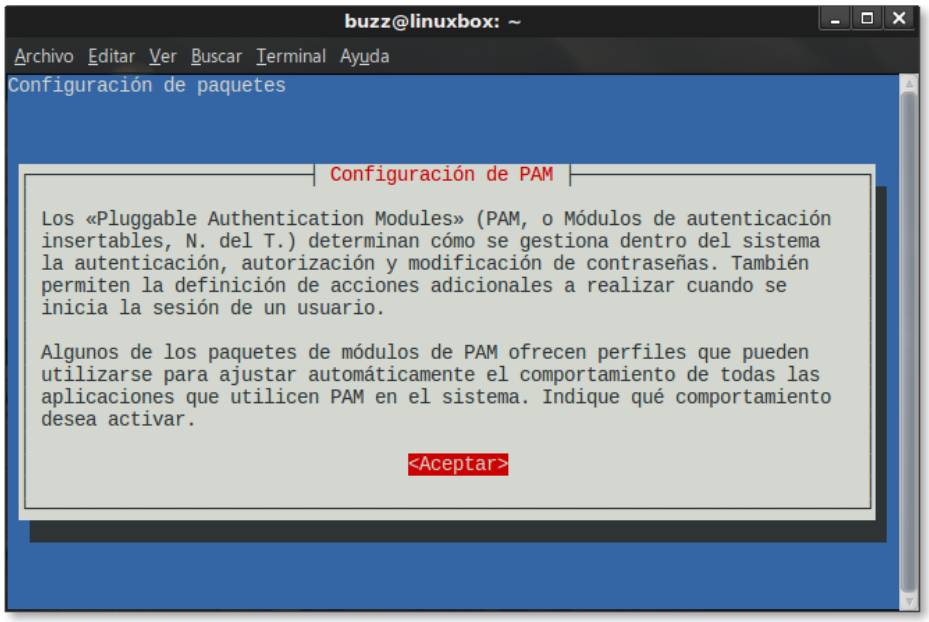
```
PermitRootLogin yes
```

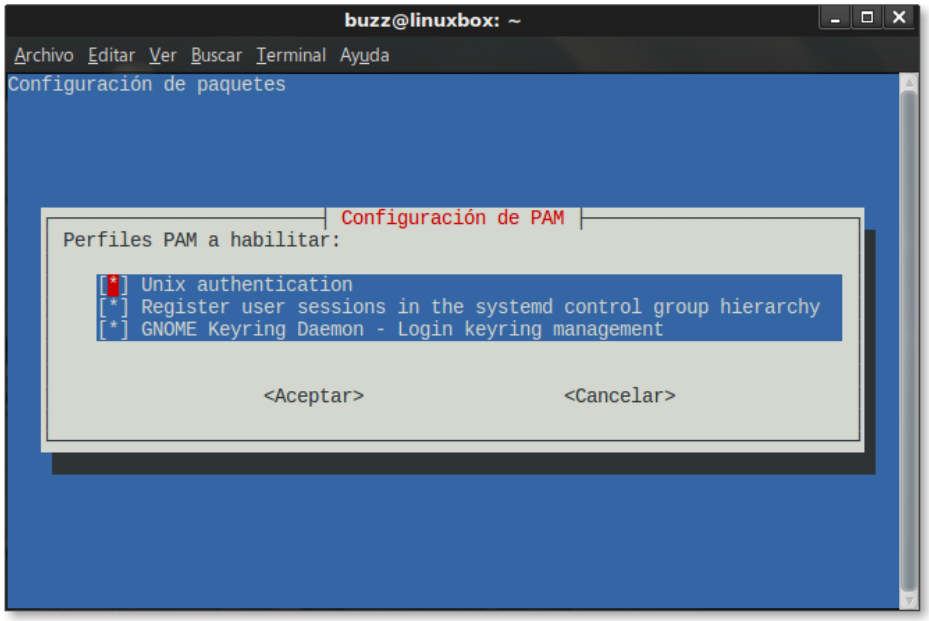
y posteriormente reiniciar y comprobar el estado del servicio mediante:

```
root@master:~# systemctl restart ssh
root@master:~# systemctl status ssh
```

Debian con el escritorio LXDE

Continuamos con el mismo equipo -cambiamos su nombre o *hostname* por "**linuxbox**" para usarlo en un futuro- al cual terminamos de instalar el Escritorio LXDE. Ejecutemos *pam-auth-update* y obtendremos las siguientes salidas:





El sistema ya habilitó todos los Perfiles -Módulos- necesarios para la correcta autenticación durante la instalación del escritorio LXDE, que a saber son los siguientes:

- Módulo de Autenticación UNIX.

- Módulo que registra las sesiones de usuarios en el Grupo Jerárquico de Control del ***systemd***.
- Módulo del Demonio GNOME Keyring

- *Aprovechamos la ocasión para recomendar que en todos los casos, cuando se nos pregunte "Perfiles PAM a habilitar", seleccionemos la opción <Cancelar> a menos que sepamos muy bien qué es lo que estamos haciendo. Si cambiamos la configuración PAM que de forma automática la hace el propio Sistema Operativo, podemos fácilmente inhabilitar el inicio de sesión en el equipo.*

En los casos anteriores estamos hablando de **Autenticación Local** o de Autenticación frente al equipo local como sucede cuando iniciamos una sesión remota mediante *ssh*.

Si implementamos un método de ***Autenticación Remota en el Equipo Local*** para que usuarios con sus Credenciales almacenadas en un servidor remoto OpenLDAP o en un Active Directory, el sistema tomará en cuenta la nueva forma de autenticación y adicionará los módulos PAM necesarios.

Archivos principales

- */etc/passwd*: Información de las Cuentas de Usuarios
- */etc/shadow*: Información Segura de las Cuentas de Usuarios
- */etc/pam.conf*: Archivo que solo debe utilizarse sino existe el directorio */etc/pam.d/*
- */etc/pam.d/*: Directorio donde los programas y servicios instalan sus módulos PAM
- */etc/pam.d/passwd*: Configuración PAM para *passwd*.
- */etc/pam.d/common-account*: Parámetros de Autorización comunes a todos los servicios
- */etc/pam.d/common-auth*: Parámetros de Autenticación comunes a todos los servicios
- */etc/pam.d/common-password*: Módulos PAM comunes a todos los servicios relacionados con las contraseñas - *passwords*
- */etc/pam.d/common-session*: Módulos PAM comunes a todos los servicios relacionados con las sesiones de usuarios
- */etc/pam.d/common-session-noninteractive*: Módulos PAM comunes a todos los servicios relacionados con las sesiones no interactivas o que no requieren de la intervención del usuario, como las tareas que se ejecutan al comienzo y final de sesiones no interactivas.
- */usr/share/doc/passwd/*: Directorio de documentación.

Recomendamos leer las páginas del manual de *passwd* y *shadow* mediante *man passwd* y *man shadow*. También es saludable leer el contenido de los archivos *common-account, common-auth, common-passwrod, common-session* y *common-session-noninteractive*.

Módulos PAM disponibles

Para tener una idea de los módulos PAM disponibles *a priori* en el repositorio estándar de Debian, ejecutamos:

```
buzz@linuxbox:~$ aptitude search libpam
```

La lista es larga y solamente reflejaremos los módulos que muestran lo extensa que es:

```
libpam-afs-session          - PAM module to set up a PAG and obtain AFS tokens
libpam-alreadyloggedin      - PAM module to skip password authentication for logged users
libpam-apparmor             - changehat AppArmor library as a PAM module
libpam-barada               - PAM module to provide two-factor authentication based on HOTP
libpam-blue                 - PAM module for local authenticaction with bluetooth devices
libpam-ca                   - POSIX 1003.1e capabilities (PAM module)
libpam-ccreds               - Pam module to cache authentication credentials
libpam-cgrou                - control and monitor control groups (PAM)
libpam-chroot               - Chroot Pluggable Authentication Module for PAM
libpam-ck-connector         - ConsoleKit PAM module
libpam-cracklib             - PAM module to enable cracklib support
libpam-dbus                 - A PAM module which asks the logged in user for confirmation
libpam-duo                  - PAM module for Duo Security two-factor authentication
libpam-dynalogin            - two-factor HOTP/TOTP authentication - implementation libs
libpam-encfs                - PAM module to automatically mount encfs filesystems on login
libpam-fprintd              - PAM module for fingerprint authentication trough fprintd
libpam-geo                  - PAM module checking access of source IPs with a GeoIP database
libpam-gnome-keyring        - PAM module to unlock the GNOME keyring upon login
libpam-google-authenticator - Two-step verification
libpam-heimdal              - PAM module for Heimdal Kerberos
libpam-krb5                 - PAM module for MIT Kerberos
libpam-krb5-migrate-heimdal - PAM module for migrating to Kerberos
libpam-lda                  - Pluggable Authentication Module for LDA
libpam-ldapd                - PAM module for using LDAP as an authentication service
libpam-mkhomedir            -
libpam-mklocaluser          - Configure PAM to create a local user if it do not exist already
```

```
libpam-modules              - Pluggable Authentication Modules for PAM
libpam-modules-bin          - Pluggable Authentication Modules for PAM - helper binaries
libpam-mount                - PAM module that can mount volumes for a user session
libpam-mysql                - PAM module allowing authentication from a MySQL server
libpam-nufw                 - The authenticating firewall [PAM module]
libpam-oath                 - OATH Toolkit libpam_oath PAM module
libpam-ocaml                - OCaml bindings for the PAM library (runtime)
libpam-openafs-kaserver     - AFS distributed filesystem kaserver PAM module
libpam-otpw                 - Use OTPW for PAM authentication
libpam-p11                  - PAM module for using PKCS#11 smart cards
libpam-passwdqc             - PAM module for password strength policy enforcement
libpam-pgsql                - PAM module to authenticate using a PostgreSQL database
libpam-pkcs11               - Fully featured PAM module for using PKCS#11 smart cards
libpam-pold                 - PAM module allowing authentication using a OpenPGP smartcard
libpam-pwdfile              - PAM module allowing authentication via an /etc/passwd-like file
libpam-pwquality            - PAM module to check password strength
libpam-python               - Enables PAM modules to be written in Python
libpam-python-doc           - Documentation for the bindings provided by libpam-python
libpam-radius-auth          - The PAM RADIUS authentication module
libpam-runtime              - Runtime support for the PAM library
libpam-script               - PAM module which allows executing a script
libpam-shield               - locks out remote attackers trying password guessing
libpam-shish                - PAM module for Shishi Kerberos v5
libpam-slurm                - PAM module to authenticate using the SLURM resource manager
libpam-smbpass              - pluggable authentication module for Samba
libpam-snapper              - PAM module for Linux filesystem snapshot management tool
libpam-ssh                  - Authenticate using SSH keys
libpam-sshauth              - authenticate using an SSH server
libpam-sss                  - Pam module for the System Security Services Daemon
libpam-systemd              - system and service manager - PAM module
libpam-tacplus              - PAM module for using TACACS+ as an authentication service
libpam-tmpdir               - automatic per-user temporary directories
libpam-usb                  - PAM module for authentication with removable USB block devices
libpam-winbind              - Windows domain authentication integration plugin
libpam-yubico               - two-factor password and YubiKey OTP PAM module
libpam0g                    - Pluggable Authentication Modules library
libpam0g-dev                - Development files for PAM
libpam4j-java               - Java binding for libpam.so
libpam4j-java-doc           - Documentation for Java binding for libpam.so
```

Saque Usted sus propias conclusiones.

CentOS

Si durante el proceso de instalación seleccionamos la opción "*Servidor con GUI*", obtendremos una buena plataforma para implementar diferentes servicios para la Red PYME. A diferencia de Debian, CentOS/Red Hat® ofrece una serie de herramientas de consola y gráficas que le hacen la vida mas fácil a un Administrador de Sistemas o de Redes.

Documentación

Instalada por defecto, la encontramos en el directorio:

```
[root@linuxbox ~]# ls -l /usr/share/doc/pam-1.1.8/
total 256
-rw-r--r--. 1 root root   2045 jun 18  2013 Copyright
drwxr-xr-x. 2 root root   4096 abr  9 06:28 html
-rw-r--r--. 1 root root 175382 nov  5 19:13 Linux-PAM_SAG.txt
-rw-r--r--. 1 root root  67948 jun 18  2013 rfc86.0.txt
drwxr-xr-x. 2 root root   4096 abr  9 06:28 txts
```

```
[root@linuxbox ~]# ls /usr/share/doc/pam-1.1.8/txts/
README.pam_access    README.pam_exec       README.pam_lastlog    README.pam_namespace   README.pam_selinux     README.pam_timestamp
README.pam_console   README.pam_faildelay  README.pam_limits     README.pam_nologin     README.pam_sepermit    README.pam_tty_audit
README.pam_cracklib  README.pam_faillock   README.pam_listfile   README.pam_permit      README.pam_shells      README.pam_umask
README.pam_chroot    README.pam_filter     README.pam_localuser  README.pam_postgresok  README.pam_stress      README.pam_unix
```

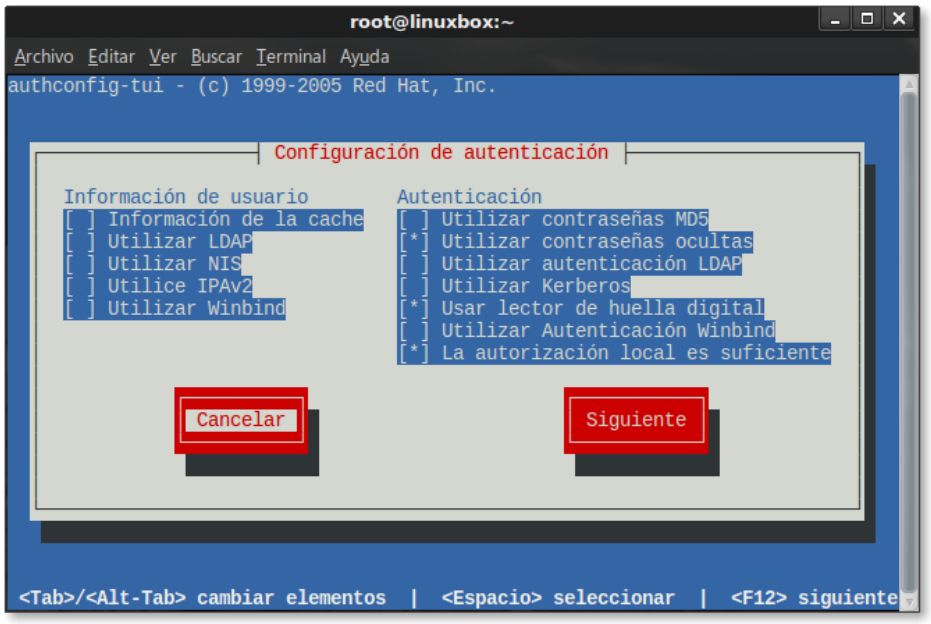
```
README.pam_debug      README.pam_ftp        README.pam_loginuid   README.pam_pwhistory   README.pam_succeed_if  README.pam_userdb
README.pam_deny       README.pam_group      README.pam_mail       README.pam_rhosts      README.pam_tally       README.pam_warn
README.pam_echo       README.pam_issue      README.pam_mkhomedir  README.pam_rootok      README.pam_tally2      README.pam_wheel
README.pam_env        README.pam_keyinit    README.pam_motd       README.pam_securetty   README.pam_time        README.pam_xauth
```

Si, también denominamos "linuxbox" al equipo CentOS al igual que con Debian, el cual nos servirá para futuros artículos sobre Redes PYMES.

CentOS con GUI GNOME3

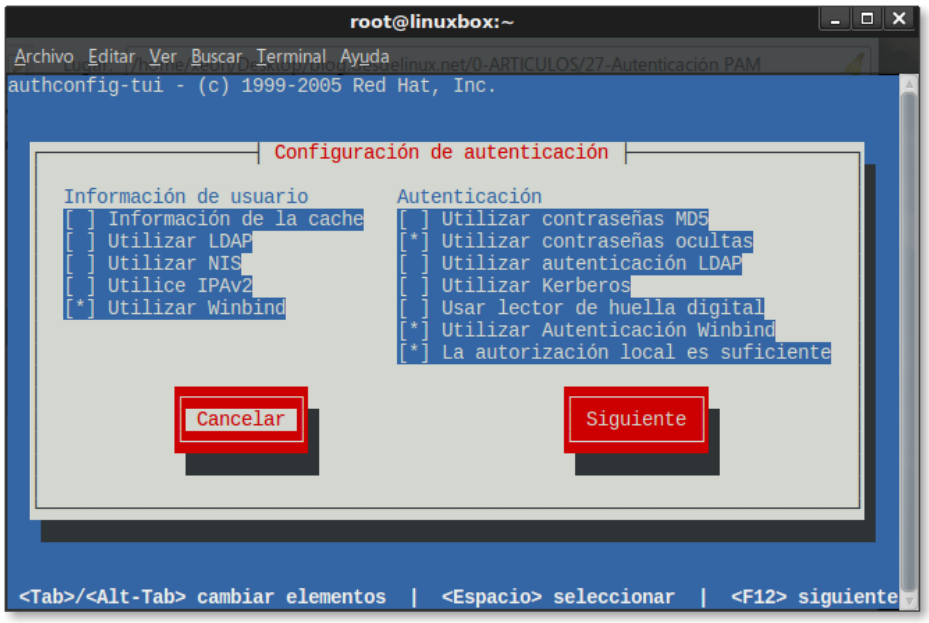
Cuando seleccionamos durante la instalación la opción "*Servidor con GUI*", se instala el Escritorio GNOME3 y demás utilidades y programas base para desarrollar un servidor. A nivel de consola, para conocer el estado de la autenticación ejecutamos:

```
[root@linuxbox ~]# authconfig-tui
```



Comprobamos que solo están habilitados los módulos PAM necesarios para la configuración actual del servidor, incluso hasta un módulo para leer huellas digitales, sistema de autenticación que encontramos en algunos modelos de Laptops.

CentOS con GUI GNOME3 unido a un Microsoft Active Directory



Como podemos comprobar, se han añadido y habilitado los módulos necesarios -*winbind*- para la autenticación frente a un Active Directory, mientras que a propósito inhabilitamos el módulo para leer huellas dactilares, porque no es necesario.

En un próximo artículo abordaremos en detalle el cómo unir un cliente CentOS 7 a un Microsoft Active Directory. Solamente adelantamos que mediante la herramienta *authoconfig-gtk* se automatiza tremendamente la instalación de paquetes necesarios, configuración de la creación automática de los directorios de usuarios del dominio que se autentiquen localmente, y el proceso en si mismo de unir el cliente al Dominio de un Active Directory. Acaso después de la unión, solo será necesario reiniciar el equipo.

Archivos principales

Los archivos relacionados con la Autenticación en CentOS se ubican en el directorio */etc/pam.d/*:

```
[root@linuxbox ~]# ls /etc/pam.d/
atd                     liveinst          smartcard-auth-ac
authconfig              login             smtp
authconfig-gtk          other             smtp.postfix
authconfig-tui          passwd            sshd
config-util             password-auth     su
crond                   password-auth-ac  sudo
cups                    pluto             sudo-i
chfn                    polkit-1          su-l
chsh                    postlogin         system-auth
fingerprint-auth        postlogin-ac      system-auth-ac
fingerprint-auth-ac     ppp               system-config-authentication
gdm-autologin           remote            systemd-user
gdm-fingerprint         runuser           vlock
gdm-launch-environment  runuser-l         vmtoolsd
gdm-password            samba             xserver
gdm-pin                 setup
gdm-smartcard           smartcard-auth
```

Módulos PAM disponibles

Tenemos los repositorios ***base, centosplus, epel,*** y ***updates***. En ellos encontramos -entre otros más- los siguientes módulos mediante los comandos *yum search pam-*, *yum search pam_*, y *yum search libpam*:

```
nss-pam-ldapd.i686 : An nsswitch module which uses directory servers
nss-pam-ldapd.x86_64 : An nsswitch module which uses directory servers
ovirt-guest-agent-pam-module.x86_64 : PAM module for the oVirt Guest Agent
pam-kwallet.x86_64 : PAM module for KWallet
```

```
pam_afs_session.x86_64 : AFS PAG and AFS tokens on login
pam_krb5.i686 : A Pluggable Authentication Module for Kerberos 5
pam_krb5.x86_64 : A Pluggable Authentication Module for Kerberos 5
pam_mapi.x86_64 : PAM module for authentication via MAPI against a Zarafa server
pam_oath.x86_64 : A PAM module for pluggable login authentication for OATH
pam_pkcs11.i686 : PKCS #11/NSS PAM login module
pam_pkcs11.x86_64 : PKCS #11/NSS PAM login module
pam_radius.x86_64 : PAM Module for RADIUS Authentication
pam_script.x86_64 : PAM module for executing scripts
pam_snapper.i686 : PAM module for calling snapper
pam_snapper.x86_64 : PAM module for calling snapper
pam_ssh.x86_64 : PAM module for use with SSH keys and ssh-agent
pam_ssh_agent_auth.i686 : PAM module for authentication with ssh-agent
pam_ssh_agent_auth.x86_64 : PAM module for authentication with ssh-agent
pam_url.x86_64 : PAM module to authenticate with HTTP servers
pam_wrapper.x86_64 : A tool to test PAM applications and PAM modules
pam_yubico.x86_64 : A Pluggable Authentication Module for yubikeys
libpamtest-doc.x86_64 : The libpamtest API documentation
python-libpamtest.x86_64 : A python wrapper for libpamtest
libpamtest.x86_64 : A tool to test PAM applications and PAM modules
libpamtest-devel.x86_64 : A tool to test PAM applications and PAM modules
```

Resumen

Es importante tener un mínimo de conocimientos sobre PAM si queremos entender de forma general como se efectúa la Autenticación cada vez que iniciamos sesión en nuestro equipo Linux/UNIX. También es importante conocer que solamente con Autenticación Local podemos brindar servicios a otros equipos en una pequeña red PYME como Proxy, Correo, FTP, etcétera, concentrados todos en un solo servidor. Todos los servicios anteriores -y muchos mas como vimos anteriormente- tienen su módulo PAM.

Fuentes consultadas

- Manuales de los comandos - *man pages*.
- Autenticación: página de Wikipedia en español
- Pluggable Authentication Modules
- Red_Hat_Enterprise_Linux-6-Deployment_Guide-en-US

¡Hasta el próximo artículo!