Configuración de la autenticación del sistema

Diego Martín Arroyo

21 de abril de 2015

Índice

Introducción

La infraestructura en la que se integra el sistema a construir cuenta con un sistema de usuarios centralizado en un servidor *LDAP* (*Lightweight Directory Access Protocol*), que posibilita el almacenamiento centralizado de la información de todos los usuarios de la infraestrucutra, y que, combinado con otros componentes, permite la utilización de una única cuenta en cualquiera de los equipos de la misma. Este sistema proporciona una serie de ventajas: delega la gestión de los usuarios al sistema central y evita la creación de nuevas cuentas para cada usuario, evitando el procesado de una cantidad de usuarios significativa.
Es por ello que el sistema contará con un cliente **LDAP** en cada uno de los nodos para poder acceder a la cuenta de cada usuario.

LDAP

El protocolo abierto **LDAP** se basa en una arquitectura cliente-servidor. En dicha arquitectura, el servidor gestiona un directorio de usuarios con una serie de datos de relevancia, tales como el par de claves usuario-contraseña, nombre completo, directorio de inicio, *shell* por defecto, etcétera. La versión actual del protocolo (versión 3) se define en [1]

Servidor a utilizar

El servidor **LDAP** presente en la infraestructura utiliza una configuración estándar accesible desde la URI `ldap://ldap1.cie.aulas.usal.es`. No utiliza autenticación por TLS *Transport Layer Security* y opera en el puerto por defecto del protocolo, el 389.

Configuración

El proceso de configuración es sencillo, y se limita a la instalación de varios paquetes y la modificación de una serie de ficheros de configuración.

```
pacman -S openldap nss-pam-ldapd
```

Para confirmar que la instalación se ha realizado de forma correcta es posible realizar consultas al servidor desde la línea de comandos:

```
ldapsearch -x -D uid=<id>,ou=people,dc=DIA -W -H ldap://ldap1.cie.aulas.usal.es:389 -b dc=dia
-s sub uid=<id>
```

Si al introducir la contraseña el comando retorna la información sobre el usuario, la autenticación se ha realizado de forma exitosa. En caso contrario se retornará un código de error.
La información que provee el directorio es la siguiente:

En primer lugar es necesario realizar la configuración del propio cliente LDAP para poder realizar consultas al mismo, que después serán aprovechadas por otros componentes.

Listing 1: Archivo `/etc/openldap/ldap.conf`

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.
```

```
BASE    dc=DIA,ou=people
URI     ldap://ldap1.cie.aulas.usal.es
```

La configuración puede probarse con el siguiente comando:

```
ldapsearch -x '(objectclass=*)'
```

Configuración del *Name Service Switch*

Un **NSS** define un conjunto de fuentes (archivos de configuración como `/etc/passwd`, servidores externos (*LDAP*)) para bases de datos de configuración. Para incluir el **LDAP** como fuente de datos únicamente es necesario modificar los ficheros de configuración del mismo:

Listing 2: Archivo `/etc/nsswitch.conf`

```
# Begin /etc/nsswitch.conf

passwd: files ldap
group: files ldap
shadow: files ldap

publickey: files

hosts: files dns myhostname
networks: files

protocols: files
services: files
ethers: files
rpc: files

netgroup: files

# End /etc/nsswitch.conf
```

En el archivo `nsswitch` se incluse información como fuentes de información los archivos del sistema (`passwd`, `gpasswd`...) y el protocolo **LDAP**

Listing 3: Archivo `/etc/nslcd.conf`

```
# This is the configuration file for the LDAP nameservice
```

El archivo contiene la información de acceso al servidor **LDAP**.
Una vez modificados los archivos según lo indicado, es posible comenzar a utilizar el servidor **LDAP** como método de autenticación. Para ello es necesario únicamente iniciar el servicio `nslcd` utilizando **systemd**:

```
systemctl start nslcd
```

Para comprobar el correcto funcionamiento del sistema, es posible utilizar el comando `getent passwd`, que en caso que la configuración se haya aplicado correctamente, mostrará todos los usuarios presentes en el servidor **LDAP**.

Configuración del módulo PAM

El *Pluggable Authentication Module* (**PAM**) es un módulo que permite realizar operaciones de autenticación y gestión de sesiones y contraseñas[2] utilizando un diseño modular y "conectable" (*pluggable*), que permite su modificación y reemplazo de forma sencilla. En **Arch Linux** el paquete que lo incluye es `nss-pam-ldapd` [3].
En general, la configuración de **PAM** consiste en añadir a los archivos de configuración presentes una serie de directivas que realicen la consulta al fichero **LDAP**. Dichos ficheros se encuentran en la ruta `/etc/pam.d`

Listing 4: Fichero `pam.d/system-auth`

```
#%PAM-1.0
auth            sufficient      pam_ldap.so
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth           sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth           required        pam_wheel.so use_uid
auth            required        pam_unix.so use_first_pass
account         sufficient      pam_ldap.so
account         required        pam_unix.so
session         sufficient      pam_ldap.so
session         required        pam_unix.so
```

Listing 5: Ficheros `pam.d/su` y `pam.d/su-l` (su contenido es idéntico en este paso)

```
#%PAM-1.0
auth            sufficient      pam_ldap.so
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth           sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth           required        pam_wheel.so use_uid
auth            required        pam_unix.so use_first_pass
account         sufficient      pam_ldap.so
account         required        pam_unix.so
session         required        pam_mkhomedir.so skel=/etc/skel umask=0022
session         sufficient      pam_ldap.so
session         required        pam_unix.so
```

Listing 6: Fichero `pam.d/passwd`

```
#%PAM-1.0
password        sufficient      pam_ldap.so
#password       required        pam_cracklib.so difok=2 minlen=8 dcredit=2 ocredit=2 retry=
#password       required        pam_unix.so sha512 shadow use_authtok
password        required        pam_unix.so sha512 shadow nullok
```

Creación del directorio de inicio

Debido a que el directorio de inicio no entra dentro del conjunto de directorios compartidos del sistema, es necesario crearlo en caso de que el usuario acceda por primera vez al sistema.

Listing 7: Fichero `pam.d/system-login`

```
#%PAM-1.0

auth        required    pam_tally.so          onerr=succeed file=/var/log/faillog
auth        required    pam_shells.so
auth        requisite   pam_nologin.so
auth        include     system-auth

account     required    pam_access.so
account     required    pam_nologin.so
account     include     system-auth

password    include     system-auth

session     optional    pam_loginuid.so
session     include     system-auth
session     optional    pam_motd.so           motd=/etc/motd
session     optional    pam_mail.so           dir=/var/spool/mail standard quiet
-session    optional    pam_systemd.so
session     required    pam_env.so
session     required    pam_mkhomedir.so skel=/etc/skel umask=0022
```

Listing 8: Fichero `pam.d/su-l` (obsérvese la línea de diferencia con `pam.d/su`)

```
#%PAM-1.0
auth            sufficient      pam_ldap.so
auth            sufficient      pam_rootok.so
# Uncomment the following line to implicitly trust users in the "wheel" group.
#auth           sufficient      pam_wheel.so trust use_uid
# Uncomment the following line to require a user to be in the "wheel" group.
#auth           required        pam_wheel.so use_uid
auth            required        pam_unix.so use_first_pass
account         sufficient      pam_ldap.so
account         required        pam_unix.so
session         required        pam_mkhomedir.so skel=/etc/skel umask=0022
session         sufficient      pam_ldap.so
session         required        pam_unix.so
```

Sin embargo esto no es suficiente para proporcionar una experiencia de uso óptima, pues la configuración descrita anteriormente no crea el directorio en el resto de nodos del sistema, obligando al usuario a iniciar sesión en cada uno de ellos para contar con un directorio de trabajo propio. Para solucionar este problema es posible utilizar un servicio de `MarcoPolo`.

También es posible dar acceso al superusuario o permitir el acceso sin conexión al servidor, de nuevo mediante parámetros de configuración.

Una vez que toda la configuración ha sido probada es posible ejecutar el comando `systemctl enable nslcd` para arrancar el sistema de autenticación cada vez que el equipo arranque.

Referencias

[1] J. Sermersheim, "Lightweight Directory Access Protocol (LDAP): The Protocol." RFC 4511 (Proposed Standard), June 2006.

[2] V. Samar and R. J. S. III, "UNIFIED LOGIN WITH PLUGGABLE AUTHENTICATION MODULES (PAM)." OSF RFC 86 (Proposed Standard), Oct. 1995.

[3] A. de Jong and E. Bélanger, "nss-pam-ldapd | Arch Linux Package Search." https://www.archlinux.org/packages/community/x86_64/nss-pam-ldapd/, Oct. 2014.

[4] "LDAP authentication." https://wiki.archlinux.org/index.php/LDAP_authentication, Apr. 2015.

[5] "OpenLDAP," *Arch Linux Wiki*, Apr. 2015.

[6] S. Luttringer, "openldap | Arch Linux Package Search." https://www.archlinux.org/packages/core/x86_64/openldap/, Dec. 2014.