Sumario

Teoria: Autenticar usuaris Unix a Windows

Existeix un problema amb l'autenticació d'usuaris de Linux i UNIX amb Active Directory: els identificadors d'usuaris i grups. Internament, ni Linux ni Windows fan referència als usuaris pel nom, sinó que utilitzen els identificadors interns únics.

Els sistemes Microsoft utilitzen el SID (identificador de seguretat), que és una estructura de longitud variable que identifica sense marge d'error els diferents usuaris dins d'un domini de Windows. El SID també conté un identificador únic de domini per tal que el sistema operatiu pugui distingir entre els usuaris en diferents dominis. https://ca.wikipedia.org/wiki/Security_Identifier

En sistemes UNIX i distribucions Linux cada usuari té un identificador d'usuari (UID) que és un nombre enter de 32 bits únic en el sistema. L'àmbit de l'UID està limitat en l'equip, sense que es garanteixi que un altre usuari en una màquina diferent pugui tenir el mateix nombre enter. Això fa que un usuari ha d'iniciar sessió en cada equip on hagi de tenir accés.

Aquest problema se soluciona proporcionant autenticació de xarxa amb el sistema d'informació de xarxa (NIS) o un directori compartit d'LDAP. El sistema d'autenticació de xarxa proporciona l'UID per a l'usuari i tots els equips Linux o UNIX utilitzen aquest sistema d'autenticació compartint el mateix usuari i els identificadors de grup.

És recomanable utilitzar Active Directory per proporcionar un usuari únic i els identificadors de grup. Es pot crear un UID per a cada usuari i grup i emmagatzemar aquest identificador amb l'objecte corresponent en Active Directory, així, quan un usuari s'autentica pot cercar l'UID per a l'usuari i proporcionar-lo per al sistema operatiu com l'identificador de l'usuari intern.

Aquesta solució, però, té un inconvenient. És necessari proporcionar un mecanisme per garantir que cada usuari i grup tenen un identificador i que aquests identificadors són únics en el bosc.

Una altra estratègia per assignar identificadors és utilitzar l'identificador relatiu (RID). L'identificador relatiu és un número enter de 32 bits que identifica l'usuari dins el domini. El RID forma part del SID. La solució consisteix en extreure el RID quan l'usuari inicia la sessió i fer-lo servir com a UID intern únic. Només cal remarcar que no podreu utilitzar aquesta estratègia en aquells entorns on existeixin diversos dominis, ja que existeix la possibilitat que els usuaris de diferents dominis tinguin el mateix valor RID.

És necessari proporcionar els identificadors de Linux o UNIX per a tots els usuaris, i els grups als quals pertanyen, que poden iniciar sessió. S'han de definir valors per als atributs uidNumber i gidNumber dels usuaris i grups. No oblideu que:

* Els sistemes UNIX i distribucions Linux necessiten un UID para a cadascun dels usuaris que autentiquen. Cada compte d'usuari que iniciarà una sessió en un equip Linux o UNIX ha de tenir un atribut uidNumber únic. El valor específic que utilitzi per a un uidNumber no és important, però ha de ser únic entre tots els usuaris que poden iniciar sessió en l'equipo de Linux o UNIX.

* Cada usuari de Linux també ha de tenir un identificador de grup predeterminat, per a cada usuari d'Active Directory que s'iniciarà en una sessió en un equipo Linux o UNIX requereix un valor per a l'atribut gidNumber. Aquest valor no ha de ser únic entre tots els usuaris, però ha d'identificar el grup.

* Cada grup en Active Directory ha de tenir un valor únic per a l'atribut gidNumber.

Teoria: Maneres de connectar Linux amb Active Directory

You need two components to connect a Linux system to Active Directory (AD). One component interacts with the central identity and authentication source, which is AD in this case. The other component detects available domains and configures the first component to work with the right identity source. There are different options that can be used to retrieve information and perform authentication against AD. Among them are:

Native LDAP and Kerberos PAM and NSS modules

Among these modules are nss_ldap, pam_ldap, and pam_krb5. As PAM and NSS modules are loaded into every application process, they directly affect the execution environment. With no caching, offline support, or sufficient protection of access credentials, use of the basic LDAP and Kerberos modules for NSS and PAM is discouraged due to their limited functionality.

Samba Winbind

Samba Winbind had been a traditional way of connecting Linux systems to AD. Winbind emulates a Windows client on a Linux system and is able to communicate to AD servers. The recent versions of the System Security Services Daemon (SSSD) closed a feature gap between Samba Winbind and SSSD and SSSD can now be used as a replacement for Winbind. In certain corner cases, Winbind might still be necessary to use but it is no longer the first choice in general.

System Security Services Daemon (SSSD)

The primary function of SSSD is to access a remote identity and authentication resource through a common framework that provides caching and offline support to the system. SSSD is highly configurable; it provides PAM and NSS integration and a database to store local users, as well as core and extended user data retrieved from a central server. SSSD is the recommended component to connect a Linux system with an identity server of your choice, be it Active Directory, Identity Management (IdM) in Red Hat Enterprise Linux, or any generic LDAP or Kerberos server.

The most convenient way to configure SSSD or Winbind in order to directly integrate a Linux system with AD is to use the realmd service. The realmd service automatically discovers information about accessible domains and realms and does not require advanced configuration to join a domain or realm.

Práctica paso 0: Prerrequisitos y comprobaciones

(0.1) Servidor Windows Server con ADDS y DNS , promocionado como servidor de dominio.

(0.2) El dominio se llama *lomio.org* y su nombre NetBios es *LOMIO*

(0.3) El dominio tiene un usuario *ana* y otro usuario *bob* en el grupo *alumnos*

(0.4) El servidor se llama *halcon* y su IP es la IP real + 50 , tanto si está en red interna como en modo puente. Cambia su nombre en propiedades del sistema y reinicia.

(0.5) El cliente se llama *milenario* y su IP es la IP real + 100 , tanto si está en red interna como en modo puente. Cambia su nombre en el dichero /etc/hostname y reinicia.

(0.6) El servidor de DNS tiene configuradas las entradas _kerberos, _ldap y _kpasswd de la zona.

(0.7) El cliente utiliza el servidor ADDS como servidor de DNS, es decir, que o bien en el fichero /etc/network/interfaces o bien en el applet de NetworkManager tiene configurada la IP del servidor y el dominio de búsqueda en el campo DNS. Recuerda que si tan sólo modificas el fichero /etc/resolv.conf, este puede cambiar de nuevo al reiniciar el ordenador.

En caso de que modifiques /etc/network/interfaces :

```
sudo nano /etc/network/interfaces
```

```
...
dns-nameservers   IP_servidor_DNS
dns-search        lomio.org
```

Al actualizar el servicio de red, el fichero /etc/resolv.conf debería contener:

```
cat /etc/resolv.conf
```

```
nameserver    IP_servidor_DNS
search        lomio.org
```

Prueba que funciona la red y el DNS con estos cinco pings:

```
ping IP_servidor            ( ¿funciona la red? )
ping 8.8.8.8                ( ¿funciona la salida a Internet? )
ping halcon.lomio.org       ( ¿funciona el servidor de DNS? )
ping halcon                 ( ¿correcto el dominio de búsqueda por defecto? )
ping www.google.es          ( ¿reenvía el sevidor de DNS ? )
```

Práctica paso 1: Instalación del software

Para poner la máquina cliente Linux como ordenador miembro del dominio Active Directory necesitaremos instalar y configurar Kerberos y Samba. Kerberos necesita NTP para sincronizar el tiempo.

Para posteriormente autentificar usuarios del dominio, necesitaremos SSSD.

```
sudo apt update
sudo apt install krb5-user ntp samba sssd
```

Práctica paso 2: Configuración de Kerberos

Durante la instalación pregunta por el nombre del reino, que es el nombre del dominio pero en mayúsculas, *LOMIO.ORG*

Podría también preguntar por el nombre del servidor (domain controller) y del gestor de identificación Kerberos (kdc) si la función de autodescubrimiento de dominio no está funcionando. En ambos casos seria *HALCON.LOMIO.ORG* , pero seguro que no será necesario.

La configuración se guarda en el fichero /etc/krb5.conf :

```
[logging]
default = FILE:/var/log/krb5.log

[libdefaults]
default_realm = LOMIO.ORG
ticket_lifetime = 24h
renew_lifetime = 7d
dns_lookup_realm = true
dns_lookup_kdc = true
rdns = false
forwardable = true

[realms]
LOMIO.ORG = {
   kdc = HALCON.LOMIO.ORG
   admin_server = HALCON
   default_domain = LOMIO
}
```

En dicho fichero establecemos un fichero de logs para poder consultar si fallase la identificación. En cambio, la sección en gris [realms] no hace falta establecerla si en SSSD se utiliza la opción auto-discovery.

Kerberos necesita que el reloj del cliente y del servidor de identificación estén sincronizados, sin desfases de tiempo. Por eso queremos que el servidor reciba la hora de Internet, y que el cliente reciba la hora del servidor de identificación o, como mucho, de la misma fuente de Internet de la que la recibe el servidor. Para ello editarás el fichero /etc/ntp.conf para añadir:

```
server = halcon.lomio.org
```

Después de realizar los cambios anteriores en los ficheros de configuración, reiniciaremos los servicios para que integren los cambios:

```
sudo systemctl restart ntp.service
```

Para aprender un poco más de Kerberos y de cómo configurarlo recomiendo los siguientes enlaces:

- https://www.howtoforge.com/how-to-setup-kerberos-server-and-client-on-ubuntu-1804-lts/

- https://web.mit.edu/kerberos/krb5-latest/doc/user/index.html

- https://web.mit.edu/kerberos/krb5-latest/doc/admin/index.html

Práctica paso 3: Configuración de Samba

Aunque no se compartan ficheros ni impresoras, se usará NetBios para la identificación en Active Directory. Para ello edita el fichero /etc/samba/smb.conf :

```
[global]
workgroup = LOMIO
client signing = yes
client use spnego = yes
kerberos method = secrets and keytab
realm = LOMIO.ORG
security = ads
log file = /var/log/samba/log.%m
password server = HALCON.LOMIO.ORG

# Para especificar si el UID y GID Unix del usuario están puestos a
# mano en el directorio (ad) o si se mapean a partir del SID (rid)
; idmap backend = rid
```

Después de realizar los cambios anteriores en los ficheros de configuración, reiniciaremos los servicios para que integren los cambios:

```
sudo systemctl restart smbd.service nmbd.service
```

Práctica paso 4: Unir el ordenador cliente al directorio

Modifica el fichero /etc/hosts para añadir el FQDN del cliente, que será necesario para que el servidor de DNS automáticamente cree una entrada para la máquina cliente cuando se integre en el dominio, así cómo para las actualizaciones de DNS dinámico cada vez que el cliente reinicie:

```
127.0.0.1       localhost
IPreal+100      milenario.lomio.org     milenario
```

Vamos a obtener un tíquet Kerberos. Para ello necesitamos el nombre del usuario con permisos administrativos en el Windows Server. En mi caso es *Administrator* :

```
sudo kinit Administrator
sudo klist
```

Si no tuviéramos la línea default_realm en el fichero /etc/krb5.conf, entonces la petición de tíquet anterior la hubiéramos escrito “sudo kinit *Administrator*@LOMIO.ORG”.

Ahora que tenemos un tíquet, antes de que caduque, vamos a unir la máquina cliente:

```
sudo net ads join -k
sudo klist -ke
```

Al unir la máquina cliente, el tíquet se guardará en el fichero /etc/krb5.keytab .

Si no funciona podemos probar especificando un usuario con permiso para añadir ordenadores:

```
sudo net ads join -k -U Administrator
sudo net ads join -k -U Administrator@LOMIO.ORG
```

Si no funciona también podemos intentar generar más mensajes para saber qué pasa:

```
sudo net ads join -k --debuglevel=1
sudo cat /var/log/samba/nmbd.log
```

Puedes comprobar que ha añadido la máquina en el dominio Active Directory revisando esto:

a) “Windows Server → Tools → Active Directory Users and Computers → Computers” muestra la nueva máquina.

b) “Windows Server → Tools → DNS → Forward Lookup Zones → lomio.org” muestra la nueva máquina.

c) Prueba a ejecutar los siguientes comandos:

```
net ads info
net ads lookup
net ads status
```

d) Prueba una búsqueda en Active Directory:

```
sudo ldapsearch -H ldap://halcon.lomio.org:3268 -Y GSSAPI -N -b
"dc=lomio,dc=org" "(objectClass=user)"
```

Práctica paso 5: Configuración de SSSD

En Ubuntu 16.04 al instalar SSSD se crea el directorio /etc/sssd/ pero no el fichero con la configuración. Crea uno que será /etc/sssd/sssd.conf , con propietario root y permisos 600 :

```
[sssd]
services = nss, pam, pac
config_file_version = 2
domains = LOMIO.ORG

[domain/LOMIO.ORG]
id_provider = ad
access_provider = ad
```

```
auth_provider = ad
chpass_provider = ad

# This example specifies /home/DOMAIN-FQDN/user as $HOME.
# Por ej, el directorio de ana estaria en /home/LOMIO.ORG/ana
# Use with pam_mkhomedir.so
override_homedir = /home/%d/%u

# allows users to log into the local system using cached
# information, even if the Active Directory domain is unavailable.
cache_credentials = true

# Enumeration is discouraged for performance reasons.
# enumerate = true

# Search the global catalog for POSIX attributes, rather than
# create UID:GID numbers based on the Windows SID.
# ldap_id_mapping = False
```

En Ubuntu 16.04 al instalar SSSD se modifica el fichero /etc/nsswitch.conf. Por si acaso comprueba que al menos las siguientes líneas tengan la opción de autentificar usando SSSD cuando no sean usuarios locales:

```
passwd:         compat sss
group:          compat sss
...
netgroup:       nis sss
sudoers:        files sss
```

En Ubuntu 16.04 al instalar SSSD también se modifican los ficheros /etc/pam.d/common-* , añadiendo líneas para el módulo pam-sss.so:

```
account    [default=bad success=ok user_unknown=ignore]  pam_sss.so
...
auth       [success=1 default=ignore]   pam_sss.so use_first_pass
...
password   sufficient    pam_sss.so use_authtok
...
session    optional      pam_sss.so
```

Si un usuario no tiene carpeta, se le creará automáticamente. Para ello añadir esta línea en el fichero /etc/pam.d/common-session detrás de la línea “session required pam_unix.so” :

```
session   required   pam_mkhomedir.so skel=/etc/skel/ umask=0022
```

Después de realizar los cambios anteriores en los ficheros de configuración, reiniciaremos los servicios para que integren los cambios:

```
sudo systemctl restart sssd.service
```

Práctica paso 6: Autentificar usuarios en el dominio

Con el ordenador añadido al dominio Active Directory y con SSSD configurado, prueba a ejecutar los siguientes comandos:

```
getent passwd ana
getent passwd ana@lomio.org
getent group alumnos
```

Aviso: si ejecutas el comando “getent passwd” verás que no te aparecen en la lista los usuarios *ana* y *bob* de Active Directory. Seguramente sea por que por cuestiones de rendimiento hemos comentado la línea “enumerate = true” en el fichero de configuración de SSSD.

Si funciona, autentifícate como un usuario:

```
su – ana
id ana@lomio.org
```

Si ha fallado podemos probar:

a) Obtener ayuda consultando los logs:

```
sudo cat /var/log/auth.log | grep ana
sudo journalctl -xn
```

b) Si realizamos cambios , nos interesará borrar la caché de SSSD antes de probarlos:

```
sudo rm -f /var/lib/sss/db/*
```

c) Comprueba que “Windows Server → Tools → Active Directory Users and Computers → View → Advanced Features → Computers → computador que has unido al dominio → Properties → Security” tiene los permisos “Read ...” para los “Authenticated User”

Práctica paso 7: ¿Cómo sería con REALMD?

El proceso con REALMD sustituiría des del paso 1 al paso 6. REALMD sustituye a SAMBA y configura automáticamente SSSD.

Sólo hay que instalar estos paquetes (-el último comando es para solucionar un error en packagekit en Ubuntu 16.04-) :

```
sudo apt update
sudo apt install realmd adcli
sudo apt install sssd sssd-tools libnss-sss libpam-sss samba-common-bin
sudo apt upgrade packagekit
```

Para añadir la máquina al reino escribimos:

```
sudo realm discover lomio.org
sudo realm join –U Administrator lomio.org
```

A partir de ese momento ya puedes utilizar SSSD para loguearte en Linux con usuarios del dominio.

```
su – ana
id ana@lomio.org
```

Si algo ha fallado , obtendrás mensajes adicionales con el comando:

```
sudo realm join –U Administrator lomio.org --verbose
```

Práctica paso 8: dar permisos de sudo a un grupo del dominio

Tiene sentido que si en Active Directory existe algún grupo con permisos administrativos, que los usuarios de dicho grupo puedan tener permisos administrativos sobre las máquinas Linux si se loguean en ellas. Vamos a probarlo con nuestro grupo llamado *alumnos* en el Active Directory:

```
sudo apt install libsss-sudo
sudo visudo
```

```
%alumnos   ALL=(ALL) ALL
```

Pruébalo entrando con un usuario de dicho grupo e intentando ejecutar un comando con sudo.