Informe práctica 3
Dominios en GNU/Linux

Alejandro Samarín Pérez - alu3862
José Lucas Grillo Lorenzo - alu3181

27 de mayo de 2011

Resumen

El objetivo de la práctica consiste en la utilización de los mecanismos que implementa Unix/Linux para la implementación de dominios. En concreto se hará uso de los servicios LDAP, NFS y autofs para este fin. Se plantea un caso práctico de una organización que utiliza un sistema Linux como soporte informático.

Parte I
Configuración previa

Antes de empezar a trabajar, es necesario tener en cuenta algunas consideraciones previas, especialmente si se utiliza software de virtualización para la implementación de las máquinas en este escenario. En el caso de VirtualBox, se necesita añadir una nueva interfaz de red tanto en la máquina cliente como en la servidor, con la categoría Red interna. Se ha de comprobar que como nombre de red tanto la MV servidora como la cliente tienen el mismo nombre de adaptador de red (innet). Tras realizar los pasos pertinentes, se puede comprobar el correcto funcionamiento de la red interna mediante el uso del comando "ping" desde el servidor hacia el cliente y viceversa.

Servidor

En la máquina servidora se establece la configuración IP de manera estática. Se le da IP 192.168.0.20 con máscara de red 255.255.255.0 a la interfaz de red cuya dirección MAC corresponde al adaptador de red configurado (innet). Esto se puede realizar manualmente mediante el comando ifconfig, o de forma que se ejecute al iniciar la máquina configurando un fichero /etc/sysconfig/network-scripts/ifcfg-ethX con el parámetro ONBOOT=yes.

Cliente

Aquí se debe hacer lo mismo, asignándole la IP 192.168.0.30 a la interfaz correspondiente a "Red interna" para crear una red local entre servidor y cliente.

Parte II
Instalación y configuración de OpenLDAP

Servidor

La primera acción a realizar es instalar el servicio OpenLDAP:

```
yum install openldap-servers
```

Lo siguiente es configurar OpenLDAP propiamente dicho, comenzando por la especificación de un usuario (admin) que se encargará de las tareas de administración del mismo, modificando las siguientes líneas en el fichero /etc/openldap/slapd.d/cn=config/olcDatabase={0}config.ldif:

```
olcRootDN: cn=admin,cn=config
olcRootPW: {SSHA}···
```

En el campo olcRootPW se debe especificar la password de este usuario 'admin', que ha sido generada por el comando "slappasswd" (Esto se puede automatizar usando la opcion -s tal que así: "slappasswd -s *contraseña*").

Una vez configurado el usuario 'admin', es necesario hacer lo mismo para el usuario que se encargará de gestionar el directorio OpenLDAP (Manager). Para ello, se han de modificar los siguientes campos en el fichero /etc/openldap/slapd.d/cn=config/olcDatabase={1}bdb.ldif:

```
olcSuffix: dc=aso11,dc=org
olcRootDN: cn=Manager,dc=aso11,dc=org
olcRootPW: {SSHA}···
```

Ahora, es necesario darle permisos de escritura a este usuario para que pueda modificar el directorio, así como denegar cualquier otro acceso no autorizado al mismo. Esto se realiza modificando el siguiente atributo en el fichero /etc/openldap/slapd.d/cn=config/olcDatabase={2}monitor.ldif:

```
olcAccess: {0} to *
        by dn.base='cn=Manager,dc=aso11,dc=org' write
        by * none
```

Una vez terminada la configuración de los usuarios relativos a la administración y gestión del OpenLDAP, se requiere insertar los datos de la organización. Como ayuda para esto, se hizo uso de las "migration_tools" para generar los fichero LDIF correspondientes a usuarios y grupos (teniendo en cuenta que es recomendable ajustar los campos $DEFAULT_MAIN_DOMAIN y $DEFAULT_BASE del fichero "migrate_common.ph" acordes con el esquema de la organización). Previamente, se crearon localmente los usuarios y grupos en el sistema, ya que las migration_tools extraen la información de ciertos ficheros locales y la convierten a formato LDIF.

Parte III
Autentificación por LDAP

Servidor

En este punto, lo primero que hay que realizar es iniciar el servicio *slapd*:

```
service slapd start
```

La base del directorio LDAP está compuesta por la especificación del dominio en la raíz y por dos unidades organizativas, People y Group, para agrupar a los usuarios y a los grupos respectivamente. Para añadirlos, se han creado inicialmente, y de manera local, a los citados usuarios y grupos que residirán finalmente en el directorio LDAP. De esta forma se pueden asignan los permisos adecuados a las directorios de conexión correspondientes, directorios de los proyectos, etc... que serán exportados posteriormente (Ver script anexo *"crear_usuarios_server.sh"*). A continuación se ha hecho uso de los ficheros LDIF generados con las *migration_tools* a partir de un subconjunto de los ficheros */etc/passwd* y */etc/group*. Con el siguiente comando se introducen en la BDB las entradas LDIF (también puede usarse "ldapadd"):

```
ldapmodify -x -D cn=Manager,dc=aso11,dc=org -H ldap://localhost
          -W -f <fichero LDIF>
```

En este punto ya es posible eliminar de manera local a los usuarios y grupos creados anteriormente, ya que han servido principalmente para exportar sus configuraciones al LDAP de manera sencilla gracias a las *migration_tools*, y ahora es redundante mantener la misma información en dos lugares distintos. Por último, pero no por ello menos importante, se debe detener el servicio *iptables* que gestiona el firewall de Linux, para que no bloquee las conexiones entrantes que le llegarán desde el cliente (Si bien esta no es la mejor opción, ya que se compromete la seguridad de todo el sistema al desactivar por completo el firewall; lo ideal sería añadir una regla explícita para permitir los accesos confiables).

Cliente

Para que el cliente sea capaz de loguearse contra el servidor LDAP que acabamos de configurar en lugar de contra su configuración almacenada localmente, es necesario llevar a cabo algunos pasos previos, a saber:
Se instalan, antes que nada, los siguientes paquetes:

```
yum install pam_ldap nss_ldap authconfig
```

Seguidamente se invoca al asistente *authconfig-tui* (si bien el propio manual del mismo advierte de que su uso está desaconsejado en favor de la herramienta análoga por línea de comandos *authconfig*); en él, se marcarán las opciones listadas a continuación:

- Utilizar LDAP
- Utilizar contraseñas ocultas
- Utilizar autenticación LDAP

La pantalla siguiente del asistente requiere especificar cuál es la IP del servidor LDAP contra el que se quieren realizar las autenticaciones, así como el DN de base del directorio. Se completan estos datos de esta manera:

```
Servidor:   ldap://192.168.0.20
DN Base:    dc=aso11,dc=org
```

Una vez finalizada la configuración a través del asistente, no está de más comprobar que efectivamente en el fichero */etc/nsswitch.conf* (entre otros, pero éste especialmente) se han reflejado los cambios indicados, de forma que el orden de prioridad del cliente a la hora de comprobar las credenciales del usuario cuando se loguea sea primero a través del servidor LDAP y segundo, en el caso de que éste fallara o no se pudiera establecer la conexión por algún motivo, los ficheros locales (*/etc/passwd, /etc/group...*).

Parte IV
NFS

Servidor

Una vez que han sido creados los directorios que serán exportados a los clientes (ya mencionados anteriormente: proyectos, directorios de conexión y común) y asignados los permisos pertinentes, se debe ahora configurar el servicio NFS para compartir eficazmente esta infraestructura de directorios con los clientes. En cuanto al servidor, es necesario tener corriendo los servicios *nfsd* y *mountd,* así como el servicio auxiliar *portmapper,* por lo que se levantan (en caso de que no estuvieran presentes alguno o la totalidad de ellos, se instalarían utilizando el gestor de paquetes *yum* de forma análoga a como se ha utilizado con anterioridad en el informe):

```
service mount start
service nfs start
service portmapper start
```

A continuación, se configura el fichero */etc/exports* para que cada usuario de la red interna acceda a su directorio de conexión alojado en el directorio */export/casa/* del servidor, que todos los usuarios de la red interna puedan acceder a los directorios de proyectos, y que cualquiera pueda acceder al directorio común (con permisos de red de sólo lectura, y convirtiéndose en accesos anónimos):

```
/export/casa        192.168.0.*(rw)
/export/proyectos   192.168.0.*(rw)
/export/comun       *(ro,all_squash)
```

Tras este paso, se reflejan en el sistema los cambios realizados con una llamada al comando *exportfs*:

```
exportfs -ra
```

Cliente

En el cliente apenas se necesitan ejecutar acciones para incorporar los beneficios que NFS aporta, toda vez que se encuentre instalado el paquete *nfs-util* (en caso contrario, instalarlo primero) para que el comando *mount* reconozca este tipo de sistema de ficheros. Ya comprobado esto, sólo resta crear el/los punto/s de montaje necesarios y comprobar que funciona la configuración propuesta del NFS, mediante un montaje manual:

```
mkdir /import/proyectos
mount -t nfs 192.168.0.20:/export/proyectos /import/proyectos
```

Parte V
AutoFS

La última parte de la práctica consiste en conseguir que este sistema de NFS que se ha configurado anteriormente funcione de manera automática y bajo demanda de los clientes. AutoFS nos proporciona una manera sencilla de lograr este objetivo, aunque se pueden considerar dos opciones para configurarlo: de la manera "tradicional" utilizando sus ficheros de configuración */etc/auto.master*, */etc/auto.home*, etc... en el lado del cliente o bien, aprovechando el directorio LDAP que ya está funcionando en el servidor, establecer esta misma configuración mediante entradas LDIF en la BDB del OpenLDAP.

Servidor

En el caso de decidir implementar AutoFS en la infraestructura LDAP ya creada, se debe primero modificar el esquema para incluir algunas clases nuevas que utilizará internamente AutoFS para especificar sus puntos de escucha, claves, etc... Tras ello, se puede comenzar a insertar entradas LDIF en 4 nuevas unidades organizativas: *auto.master* (donde se especificarán su vez todos los puntos de escucha), *auto.home* (para la ruta del servidor y las opciones de montaje de los directorios de conexión de los usuarios), *auto.proyectos* (ídem para los proyectos) y *auto.shared* (ídem para el directorio común). Las entradas LDIF concretas se encuentran en el anexo de este documento.

Cliente

En caso de decidirse por la opción más habitual de configuración a través de los ficheros locales, se han de modificar los ficheros equivalentes a las entradas LDIF mencionadas previamente, es decir, */etc/auto.master*, */etc/auto.home*, */etc/auto.proyectos* y */etc/auto.shared*:

/etc/auto.master Hay que añadir las siguientes líneas (y comentar las que pudieran estar activas con anterioridad):

```
/import/casa        /etc/auto.home
/import/proyectos   /etc/auto.proyectos
/import/shared      /etc/auto.shared
```

Esto significa que para cada punto de escucha especificado (/import/casa, etc...) se debe hacer uso de la configuración residente en el fichero especificado en la segunda columna.

/etc/auto.home Añadir la siguiente línea:

```
*  -fstype=nfs,rw,hard,intr,vers=3  192.168.0.20:/export/casa/&
```

/etc/auto.proyectos Añadir la siguiente línea:

```
*  -fstype=nfs,rw,hard,intr,vers=3  192.168.0.20:/export/proyectos/&
```

/etc/auto.shared Añadir la siguiente línea:

```
comun  -fstype=nfs,ro,hard,intr,vers=3  192.168.0.20:/export/shared/
```

En este caso, se indica que la clave dentro del punto de escucha */import/shared* será un único directorio denominado *"común"*.

/etc/nsswitch.conf Por último, es necesario comprobar una entrada en este fichero para asegurarse de que el servicio de automontaje buscará la configuración requerida en los ficheros locales, y no en el directorio LDAP por ejemplo:

```
automount: files ldap
```

De este modo, se asegura que la comprobación de los ficheros mencionados anteriormente tendrá preferencia sobre otras posibles opciones. Finalmente, se reinicia el servicio *autofs* para actualizar toda esta configuración.

Parte VI
Scripts anexos

crear_directorios_server.sh Se ejecuta en el servidor.

```
#!/bin/bash

mkdir -p /export/casa
mkdir -p /export/casa/irene
chmod 0770 /export/casa/irene
# 516 es el UID de irene, extraido del directorio LDAP
chgrp 516 /export/casa/irene

mkdir -p /export/casa/clara
chmod 0770 /export/casa/clara
```

```
chgrp 518 /export/casa/clara

mkdir -p /export/casa/laura
chmod 0770 /export/casa/laura
chgrp 517 /export/casa/laura

mkdir -p -m 0755 /export/comun
mkdir -p -m 0755 /export/proyectos
# Se establece bit SETGID para permitir que los nuevos ficheros/directorios
# creados hereden el grupo primario del directorio raiz
mkdir -m 2770 /export/proyectos/videojuegos
# 514 es el GID del grupo "videojuegos", extraido del directorio LDAP
chgrp 514 /export/proyectos/videojuegos
mkdir -m 2770 /export/proyectos/portales
chgrp 515 /export/proyectos/portales

# Con el uso de ACL's por defecto aseguramos que los permisos necesarios
# para que todos los miembros del grupo puedan acceder y modificar los
# ficheros creados por otros usuarios esten asignados desde su creacion
setfacl -d -m g:514:rwx /export/proyectos/videojuegos
setfacl -d -m g:515:rwx /export/proyectos/portales
```

puntos_montaje.sh Se ejecuta en el cliente.

```
#!/bin/bash

mkdir -p /import/casa
mkdir -p /import/casa/irene
chmod 0770 /import/casa/irene
chgrp 516 /import/casa/irene
mkdir -p /import/casa/clara
chmod 0770 /import/casa/clara
chgrp 518 /import/casa/clara
mkdir -p /import/casa/laura
chmod 0770 /import/casa/laura
chgrp 517 /import/casa/laura

mkdir -p -m 0755 /import/comun
mkdir -p -m 0755 /import/proyectos
mkdir -m 2770 /import/proyectos/videojuegos
chgrp 514 /import/proyectos/videojuegos
mkdir -m 2770 /import/proyectos/portales
chgrp 515 /import/proyectos/portales
```

ous.ldif Se ejecuta en el servidor.

```
dn: dc=aso11,dc=org
objectClass: dcObject
objectClass: organization
objectClass: top
o: aso11
```

```
dn: ou=People,dc=aso11,dc=org
objectClass: top
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=aso11,dc=org
objectClass: top
objectClass: organizationalUnit
ou: Group
```

users.ldif Se ejecuta en el servidor.

```
dn: uid=irene,ou=People,dc=aso11,dc=org
uid: irene
cn: irene
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$6$rOzewMjAfW/l4$cn7d7SsKJ8oOMhxT.UsfbXDEyX4HnPySVKHm...
shadowLastChange: 15103
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 509
gidNumber: 516
homeDirectory: /import/casa/irene

dn: uid=laura,ou=People,dc=aso11,dc=org
uid: laura
cn: laura
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$6$zR4DILlfzXRAJyy$NHbeWH/zQZW3XyeW7fq72c2xcWgkyhqIwMt...
shadowLastChange: 15103
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 510
gidNumber: 517
homeDirectory: /import/casa/laura

dn: uid=clara,ou=People,dc=aso11,dc=org
uid: clara
cn: clara
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$6$rI7gH/D1X7eZoq$sd9vlksjR51oKYrOfKoixsROpSulIEG5JXCHl...
shadowLastChange: 15103
```

```
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 511
gidNumber: 518
homeDirectory: /import/casa/clara
```

groups.ldif Se ejecuta en el servidor.

```
dn: cn=videojuegos,ou=Group,dc=aso11,dc=org
objectClass: posixGroup
objectClass: top
cn: videojuegos
userPassword: {crypt}x
gidNumber: 514
memberUid: clara
memberUid: irene

dn: cn=portales,ou=Group,dc=aso11,dc=org
objectClass: posixGroup
objectClass: top
cn: portales
userPassword: {crypt}x
gidNumber: 515
memberUid: clara
memberUid: laura

dn: cn=irene,ou=Group,dc=aso11,dc=org
objectClass: posixGroup
objectClass: top
cn: irene
userPassword: {crypt}x
gidNumber: 516

dn: cn=laura,ou=Group,dc=aso11,dc=org
objectClass: posixGroup
objectClass: top
cn: laura
userPassword: {crypt}x
gidNumber: 517

dn: cn=clara,ou=Group,dc=aso11,dc=org
objectClass: posixGroup
objectClass: top
cn: clara
userPassword: {crypt}x
gidNumber: 518
```

automounttree.ldif Se ejecuta en el servidor.

```
dn: ou=auto.master,dc=aso11,dc=org
ou: auto.master
```

```
objectClass: top
objectClass: automountMap

#
# Entradas para el automontaje de los directorios de conexion de los usuarios
#

dn: cn=/import/casa,ou=auto.master,dc=aso11,dc=org
cn: /import/casa
objectClass: automount
automountInformation: ldap 192.168.0.20:ou=auto.home,dc=aso11,dc=org

dn: ou=auto.home,dc=aso11,dc=org
ou: auto.home
objectClass: top
objectClass: automountMap

dn: cn=irene,ou=auto.home,dc=aso11,dc=org
cn: irene
objectClass: automount
automountInformation: -fstype=nfs,rw,hard,intr,nodev,exec,nosuid,rsize=8192,
                      wsize=8192 192.168.0.20:/export/casa/irene

dn: cn=laura,ou=auto.home,dc=aso11,dc=org
cn: laura
objectClass: automount
automountInformation: -fstype=nfs,rw,hard,intr,nodev,exec,nosuid,rsize=8192,
                      wsize=8192 192.168.0.20:/export/casa/laura

dn: cn=clara,ou=auto.home,dc=aso11,dc=org
cn: clara
objectClass: automount
automountInformation: -fstype=nfs,rw,hard,intr,nodev,exec,nosuid,rsize=8192,
                      wsize=8192 192.168.0.20:/export/casa/clara

#
# Entradas para el automontaje de los directorios de los proyectos
#

dn: ou=auto.proyectos,dc=aso11,dc=org
ou: auto.proyectos
objectClass: top
objectClass: automountMap

dn: cn=/import/proyectos,ou=auto.master,dc=aso11,dc=org
cn: /import/proyectos
objectClass: automount
automountInformation: ldap 192.168.0.20:ou=auto.proyectos,dc=aso11,dc=org

dn: cn=videojuegos,ou=auto.proyectos,dc=aso11,dc=org
cn: videojuegos
objectClass: automount
automountInformation: -fstype=nfs,rw,hard,intr,nodev,exec,nosuid,rsize=8192,
                      wsize=8192 192.168.0.20:/export/proyectos/videojuegos
```

```
dn: cn=portales,ou=auto.proyectos,dc=aso11,dc=org
cn: portales
objectClass: automount
automountInformation: -fstype=nfs,rw,hard,intr,nodev,exec,nosuid,rsize=8192,
                      wsize=8192 192.168.0.20:/export/proyectos/portales

#
# Entradas para el automontaje del directorio comun
#

dn: ou=auto.shared,dc=aso11,dc=org
ou: auto.shared
objectClass: top
objectClass: automountMap

dn: cn=/import/shared,ou=auto.master,dc=aso11,dc=org
cn: /import/shared
objectClass: automount
automountInformation: ldap 192.168.0.20:ou=auto.shared,dc=aso11,dc=org

dn: cn=comun,ou=auto.shared,dc=aso11,dc=org
cn: comun
objectClass: automount
automountInformation: -fstype=nfs,ro,hard,intr,nodev,exec,nosuid,rsize=8192,
                      wsize=8192 192.168.0.20:/export/shared/comun
```