ADMINISTRACIÓN DE REDES Y SISTEMAS

PRÁCTICAS DE LABORATORIO

Servicio de directorio LDAP

El servicio de directorio LDAP (*Lightweight Directory Access Protocol*, RFC 4510) se utiliza de forma habitual para compartir información sobre usuarios, equipos, aplicaciones, sistemas y otros datos de interés entre las diversas aplicaciones y sistemas de una organización. Proviene del servicio de directorio X.500, por lo que comparte muchos conceptos básicos con ese estándar.

En esta práctica se va a utilizar OpenLDAP para compartir información sobre usuarios y grupos entre sistemas de tipo POSIX.

Instalación y configuración de OpenLDAP

En primer lugar, se ha de instalar OpenLDAP y configurarlo para que permita almacenar información sobre usuarios y grupos de tipo POSIX.

Tarea 1: Instale, en la jaula 05, el paquete `openldap26-server`. Esto también instalará las herramientas de cliente y otros paquetes necesarios.

Tarea 2: Añada al fichero `/etc/rc.conf` las líneas para habilitar OpenLDAP que se indican al instalar el paquete. Si es necesario, puede verlas otra vez ejecutando:

```
pkg query %M openldap26-server.
```

NOTA: si intenta lanzar el servicio en este momento puede que obtenga un error, ya que aún hay que configurar algunos aspectos y cargar la base de datos inicial.

Tarea 3: Edite el fichero `/usr/local/etc/openldap/slapd.conf` y modifique su configuración tal como se explica en clase y se ilustra en las diapositivas. En resumen añada o verifique que ya están habilitados los siguientes aspectos:

- Añadir esquemas necesarios para clases inetOrgPerson y posixAccount.
- Habilitar base de datos mdb.
- Definir sufijo base según el dominio del alumno (dc=xxx,dc=mucs,dc=es).
- Definir superusuario y contraseña (rootdn, rootpw). Usar `slappasswd` para generar la contraseña.
- Indexar algunos atributos.
- Definir permisos de acceso a subárbol y atributos.

Utilice la orden `slaptest -u` para verificar que el fichero de configuración es válido y corrija cualquier posible error que se indique. Un error común es que, si una directiva `access` tiene cláusulas `by` en líneas posteriores, esas líneas han de empezar con un espacio o tabulador para que se considere que pertenecen a la misma directiva.

Carga de la base de datos inicial

Antes de arrancar OpenLDAP por primera vez es necesario crear la base de datos inicial. En principio basta con que tenga un contenedor base y el objeto que representa al superusuario, aunque pueden definirse también unidades organizativas, etc.

Tarea 4: Descargue la plantilla para la base de datos inicial de OpenLDAP y ajústela para su directorio.

Tarea 5: Cargue la base de datos inicial ejecutando las siguientes órdenes:

```
chown ldap /usr/local/etc/openldap/slapd.conf
su -m ldap -c 'slapadd -l inicio.ldif'
```

Tarea 6: Arranque el servidor de LDAP (`service slapd start`)

Tarea 7: Realice una búsqueda para comprobar que el servidor está operativo y devuelve el resultado esperado. Por ejemplo:

```
ldapsearch -x -L -b 'dc=xxx,dc=mucs,dc=es'
     -D 'cn=Manager,dc=xxx,dc=mucs,dc=es' -W
```

Gestión de objetos

En este apartado se pueden utilizar las herramientas de cliente para añadir, modificar, eliminar y buscar objetos. Puede utilizar los ejemplos de las diapositivas para generar los ficheros LDIF necesarios en cada caso. Tras cada operación de modificación del directorio se recomienda usar `ldapsearch` para comprobar que la información existente es la esperada.

Tarea 8: Utilice `ldapadd`, `ldappasswd`, `ldapmodify` y `ldapdelete` para crear, modificar y eliminar diversos objetos de prueba que representen a usuarios de un sistema de tipo POSIX.

Tarea 9: Utilice `ldapsearch` para hacer búsquedas con filtros.

Tarea 10: Finalmente, asegúrese de que existen en su directorio varios usuarios (posixAccount) y grupos (posixGroup) para que se puedan utilizar en las tareas posteriores.

Localización del servicio

Al igual que con otros muchos servicios, es importante que sea fácil localizar a los servidores de LDAP. Dado que normalmente los accesos al servicio comienzan por traducir algún nombre de máquina a su correspondiente dirección de red, un buen lugar para implantar mecanismos de localización es el DNS.

Una forma habitual de localizar el servicio es utilizar un nombre de DNS obvio.

Tarea 11: Añada el nombre “ldap.xxx” a su dominio de DNS para que apunte al servidor de LDAP. Puede ser un registro A que apunte directamente al servidor o bien puede ser un alias al nombre del servidor, como prefiera. Realice pruebas con cualquiera de las órdenes de las cuestiones anteriores añadiendo el argumento `-H ldap://ldap.xxx`.

Otro mecanismo más potente es utilizar registros SRV, aunque requiere que los clientes sepan utilizarlos.

Tarea 12: (Opcional) Añada los registros SRV necesarios a su dominio para que los programas clientes de LDAP de las cuestiones anteriores puedan localizar al servidor. Puede consultar esta guía para realizar la tarea.

Compartición de usuarios y grupos POSIX

Uno de los casos de uso frecuentes es tener una base de datos de usuarios y grupos compartida entre diversos equipos y sistemas. A continuación, se tratará un ejemplo de despliegue.

La idea general es que se crearán los usuarios en el directorio LDAP como objetos posixAccount y que los clientes los reconocerán por medio de ciertas bibliotecas de LDAP. Para autenticar a los usuarios los clientes comprobarán si se puede abrir sesión de LDAP con el usuario y contraseña proporcionados. Para obtener información sobre otros usuarios los clientes harán búsquedas en el directorio y leerán los atributos que necesiten. Como el directorio no permite búsquedas anónimas, los clientes usarán una cuenta reservada para estas búsquedas.

En primer lugar, se creará la cuenta reservada en el directorio LDAP.

Tarea 13: (Opción más sencilla) Cree un usuario de LDAP nuevo llamado nss_ldap.

Tarea 14: (Opción mejor) Conviene que este usuario esté diferenciado de los usuarios convencionales. Una forma de hacerlo es crear una unidad organizativa (organizationalUnit) llamada “servicios” o algo similar y luego crear en ella este tipo de cuentas. Además, el objeto para este usuario no necesita ser de la clase posixAccount/inetOrgPerson, puesto que va a ser una cuenta “pelada”; basta con que herede de las clases account y simpleSecurityObject.

Como cliente para hacer pruebas se usará una máquina diferente (también podría usarse la máquina del servidor de LDAP configurándola como cliente de sí misma). Obviamente, puede configurar múltiples clientes repitiendo los siguientes pasos en cada uno de ellos.

Tarea 15: Instale los paquetes `openldap26-client`, `pam_ldap` y `nss_ldap` en la máquina cliente. Utilice la jaula 06 como cliente.

Tarea 16: Utilice `ldapsearch` en el cliente y autenticándose con el usuario reservado para hacer alguna búsqueda de prueba, y así verificar que el cliente tiene conectividad con el directorio y el usuario reservado funciona como se esperaba.

A continuación, se va a realizar la integración de los usuarios de LDAP en la máquina cliente. Para ello es necesario configurar en el cliente los módulos PAM (*Pluggable Authentication Modules*) y NSS (*Name Service Switch*). Todas las tareas que vienen a continuación se realizan en el cliente.

IMPORTANTE: si las tareas siguientes se realizan incorrectamente, puede que la máquina cliente no reconozca a ningún usuario, ni siquiera al superusuario. Para poder recuperarse en tal caso se recomienda dejar abierta una sesión de root desde la cual podría recuperarse el sistema.

Tarea 17: Para simplificar las tareas posteriores se puede compartir la configuración de los módulos pam_ldap y nss_ldap. Para ello, en el directorio `/usr/local/etc`, cree un enlace simbólico `ldap.conf` que apunte a `nss_ldap.conf`.

Tarea 18: Edite el fichero `/usr/local/etc/ldap.conf` y modifique su configuración tal como se explica en clase y se ilustra en las diapositivas. En resumen:

- Definir el servidor de LDAP (host).
- Definir el nodo base (base).
- Definir el usuario reservado para buscar en el directorio (binddn, bindpw). Sea consciente de que el fichero donde está guardando estas credenciales será legible por cualquier usuario local.
- Especificar el comportamiento de reconexión en caso de fallo: bind_policy soft.

Tarea 19: Configure el subsistema PAM del cliente para que el servicio sshd pueda autenticar a los usuarios del directorio LDAP (edite `/etc/pam.d/sshd`) y el subsistema NSS para que los reconozca (edite `/etc/nsswitch.conf`).

Tarea 20: Para verificar que el cliente reconoce a los usuarios de LDAP, intente abrir sesiones de SSH en el cliente con las cuentas definidas en el directorio. Una vez abierta la sesión pruebe a crear ficheros en el directorio `/tmp` y use `ls -l` para verificar que el dueño y grupo son los esperados.

NOTA: al abrir las sesiones seguramente verá un mensaje que indica que el directorio personal de la cuenta no existe. Esto es normal, puesto que el directorio LDAP únicamente proporciona información sobre las cuentas de usuario, pero sus directorios no se crean automáticamente. De hecho, en un caso más completo probablemente los directorios personales de las cuentas se montarían de un servidor de ficheros.

Acceso con TLS al directorio (opcional)

El acceso al servidor de directorio puede hacerse a través de una sesión TLS para dotar al sistema de protección contra los ataques típicos a las sesiones en claro.

Tarea 21: Configure el servidor de LDAP para que admita sesiones TLS. Puede guiarse por la Guía del Administrador de OpenLDAP, por ejemplo.