Síntesis conceptual

Grado: Administración de Sistemas Informáticos en Red
Asignatura: Administración de sistemas operativos
Unidad: 4. LDAP

Resumen

Para implementar LDAP en servidores lo más usado es el AD de Windows y *OpenLDAP* en Linux. *OpenLDAP* nos permitirá crear un servicio centralizado de autentificación en nuestra estructura y crear ACL que nos permitan controlar el acceso a los recursos.

LDAP o *Lightweight Directory Access Protocol* consiste en un protocolo que funciona como una aplicación con la que se pueden llevar a cabo consultas acerca de un servicio de directorio para realizar búsquedas de información.

Una de las principales autorizaciones de LDAP en cuanto a seguridad se refiere es el *Host-Based Access Control*, que se basa en indicar en que dispositivos o *host* pueden iniciar sesión los distintos usuarios de LDAP. Para poder realizar dicha acción se añadirá la directiva *pam_check_host_attr* al fichero */etc/pam.conf*.

Para instalar *OpenLDAP*, debemos instalar los paquetes *slapd* y *ldap-utils*. Los ficheros de configuración principales se alojan en */etc /ldap*, pero a la hora de la verdad lo más práctico es usar el comando **dpkg-reconfigure slapd.** Podemos comprobar después el estado del servicio con el comando **systemctl**. Otra prueba que podemos realizar es usar el comando:

ldapwhoami -H ldap:// -x

Este comando debe devolvernos *Anonymous* como usuario para saber que todo funciona correcto. El comando que nos dirá la información de la configuración realizada anteriormente es **slapcat**. Para crear objetos en LDAP, primero debemos de definir un fichero *.ldif* con la siguiente estructura:

dn: ou=unidad_organizativa,dc=dominio,dc=dominio
objectClass: organizationalUnit
objetcClass: top
ou: unidad_organizativa
description: descripción de la unidad

Dependiendo de que queramos crear, la estructura variará más o menos, dependiendo. El comando para añadir los objetos especificados en el fichero es el siguiente:

ldapadd -c -x -D cn=admin,dc=*dominio*,dc=*dominio* -W -f *fichero.ldif*

Podemos buscar información acerca de los objetos que hemos añadido usando el comando **ldapsearch**. El comando que se encarga del borrado es **ldapdelete**. Por último, en comandos específicos de LDAP es **ldapmodify**, que puede llevar las opciones **add, replace** y **delete**.

Para poder configurar LDAP de manera gráfica, existe la herramienta *phpLdapAdmin*, que mediante la dirección *http://localhost/phpldapadmin* nos permite conectarnos una vez instalado el paquete con el mismo nombre.

Otra opción que tenemos en LDAP, es configurarlo con certificados de confianza no autofirmados usando **openssl** como comando.

Por último, tenemos las redes heterogéneas en esta unidad, que nos hablan de la versatilidad de incorporar LDAP con distintas tecnologías para tener asociados distintos tipos de sistema en una misma red.

Procesos fundamentales

Pasos para establecer un certificado válido con LDAP:

1. Establecer una nueva entidad certificadora.
2. Crear petición de firma de certificado del servidor.
3. Firmar el certificado con la autoridad certificadora.
4. Copiar los certificados a la carpeta que queramos, renombrarlos y protegerlos.
5. Configurar *slapd* para que use los certificados.
6. Modificar el script de inicio de *slapd* para que use el protocolo seguro *ldaps*.
7. Reiniciar *slapd*.

Conceptos fundamentales

- **Servicio de directorio:** aplicación o conjunto de aplicaciones que ayudan a organizar y almacenar los datos que tenemos sobre usuarios y recursos de una red.
- ***Host-Based Access Control:*** autorización basada en equipos. Es un mecanismo de LDAP que nos permite indicar en que equipos pueden iniciar sesión los distintos usuarios.
- ***OpenLDAP:*** aplicación de código abierto que nos permite gestionar el servicio de LDAP.
- **Entidad certificadora:** entidad que se encarga de firmar certificados propios para después emitirlos y poder cifrar las comunicaciones.
- **Red heterogénea:** sistema en red en el que conviven distintos sistemas multiplataforma, Linux, Windows, etc.