MEDAC
Instituto Oficial de Formación Profesional

DESPLIEGUE DE APLICACIONES WEB
TÉCNICO EN DESARROLLO DE APLICACIONES WEB

El servicio de directorio

13

ÍNDICE

 ISBN: 978-84-18983-26-9

OBJETIVOS

Descubrir qué es y para qué sirve el servicio de directorio.

Conocer cómo funciona.

Aprender a instalar servidores de directorio.

Validar usuarios de un servidor de directorio en aplicaciones web.

/ 1. Introducción y contextualización práctica

En esta unidad, analizaremos el funcionamiento, protocolos, estructura y utilidad del servicio de directorio. Este servicio nos permitirá crear una base de datos de usuarios que podremos utilizar para iniciar sesión en otras aplicaciones.

Por otro lado, explicaremos cómo instalar y configurar servidores de directorio y gestionar los objetos que albergue.

Fig. 1. El servicio de directorio.

Planteamiento del caso práctico inicial

A continuación, vamos a plantear un caso a través del cual podremos aproximarnos de forma práctica a la teoría de este tema.

Escucha el siguiente audio donde planteamos la contextualización práctica de este tema, encontrarás su resolución en el apartado Resumen y resolución del caso práctico.

Audio intro. "Caso práctico inicial"
https://bit.ly/3okAdCl

/ 2. El servicio de directorio

A medida que el acceso a un sistema o servicio crece, se generará la necesidad de autorizar una mayor cantidad de usuarios. Para almacenar y gestionar estos usuarios, podríamos utilizar, por ejemplo, una base de datos.

Un directorio es una **base de datos especializada** que almacena información y nos ofrece la posibilidad de iniciar sesión en diferentes servicios utilizando un único *login*. De esta forma, mejoramos la interoperabilidad entre sistemas y facilitamos el acceso a los recursos.

A diferencia de una base de datos de propósito general, un directorio no sufrirá demasiadas modificaciones. Esto se debe al tipo de datos almacenados: una base de datos orientada a la gestión de ventas y pedidos variará constantemente, en cambio, un listín de usuarios no se modificará con la misma frecuencia.

Un ejemplo de directorio podría ser el catálogo de libros de una biblioteca en el que la información estará clasificada según un título o código principal y el conjunto de atributos que los definen, como podría ser la fecha de publicación o nombre del autor.

Respecto a los directorios en papel, por ejemplo, un listín telefónico como las antiguas *Páginas amarillas* impresas, los directorios digitales tienen algunas ventajas:

- Optimizan la **seguridad** permitiendo seleccionar qué usuarios podrán realizar consultas y restringiendo la escritura a los usuarios con permisos de administrador.
- Permiten modificaciones y se actualizan de manera inmediata, es decir, son **dinámicos.**
- Permiten añadir nuevos campos en un registro sin afectar al resto del directorio, o sea, el servicio de directorio es **flexible.**

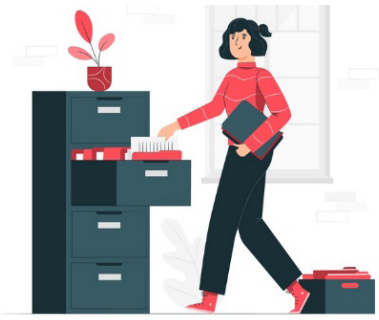

Fig. 2 Directorio en papel.

Del mismo modo que DNS se estructura en una jerarquía bajo un nombre de dominio, el servicio de directorio utiliza un FQDN para organizar los objetos que albergue. De esta manera, se crea una red de equipos y usuarios bajo un mismo sufijo DNS que facilitará encontrar recursos en una red local o en internet.

2.1. El protocolo LDAP

Dentro del listado de protocolos que trabajan sobre la capa de aplicación del módulo OSI, podemos encontrar LDAP. El servicio de directorio se basa en este protocolo para establecer conexiones **cliente-servidor.**

El protocolo LDAP *(Lighweight Directory Access Protocol)* es un estándar abierto que realiza las comunicaciones entre cliente y servidor a través del protocolo TCP/IP, utilizando el puerto **TPC 389** para conexiones estándar y el **636,** para conexiones seguras SSL (LDAPS o SLDAP).

El servicio de directorio puede establecer un modo de funcionamiento centralizado o distribuido en varios servidores. En el caso de estar distribuido, la carga de trabajo se repartirá entre los diferentes servidores pudiendo configurarse en HA *(High Availability o Alta Disponibilidad)*

LDAP aparece como una versión simple y reducida del estándar X.500, que estructura los datos de manera jerárquica y es capaz de gestionar un gran volumen de los mismos. No obstante, X.500 utiliza el protocolo **DAP** *(Directory Access Protocol)* y tanto servidor y cliente deben implementar la pila de protocolos OSI para poder comunicarse.

Estructura LDAP

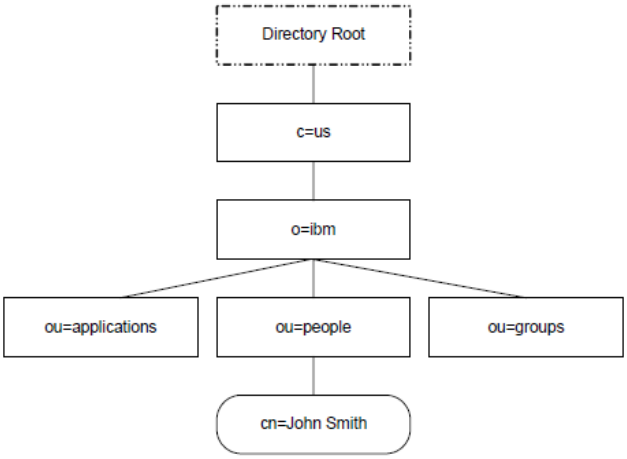

Fig. 3. Estructura LDAP. Extraído de: Understanding LDAP Design and Implementation.

Al igual que ocurre con DNS, el servicio de directorio utiliza un sistema jerárquico para definir las relaciones entre los diferentes objetos, unidades organizativas y demás atributos.

Siguiendo con la similitud con DNS, el usuario "Javier.Lopez" perteneciente al grupo 'contabilidad' del dominio "empresa.com"; en LDAP, se representaría de la siguiente forma:

```
CN=Javier.lopez,OU=contabilidad,DC=empresa,DC=com
```

Código 1. Nomenclatura LDAP para definir un DN (distinguished name).

/ 3. El formato LDIF y la implementación del servicio de directorio

a. **Formato LDIF**

Como en cualquier sistema que trabajemos con datos, podemos necesitar realizar operaciones masivas, como actualizar un campo de una gran cantidad de registros. Esto se dificulta aún más cuando no disponemos de un entorno gráfico que permita la gestión.

Para este tipo de operaciones en LDAP, podemos utilizar los ficheros LDIF *(LDAP Data Interchange Format)*. Estos ficheros nos permiten declarar todos los objetos que queramos insertar, modificar o eliminar para procesarlos en el servidor de directorio, posteriormente.

```
dn: uid=maria,ou=sistemas,dc=directorio,dc=empresa,dc=com
objectClass: inetOrgPerson
uid: Maria
sn: Bonoso
cn: Maria Bonoso
displayName: Maria Bonoso
```

Código 2. Ejemplo de un fichero LDIF para insertar datos.

Escaneando el siguiente código QR podremos acceder a la web de Oracle donde encontraremos información ampliada sobre el funcionamiento de los ficheros LDIF.

Fig. 4. Qr web Oracle.

Vídeo 1. "Gestor LDAP gráfico – LDAP Admin"
https://bit.ly/3muYrt6

b. **Implementaciones del servicio de directorio**

Del mismo modo que utilizamos Apache para desplegar servidores web sobre el protocolo HTTP, utilizaremos diferentes tipos de *software* para montar un servidor LDAP. Podemos encontrar dos grandes servidores de directorio: **OpenLDAP y Microsoft Active Directory.** OpenLDAP es un servidor LDAP Open Source para sistemas Linux. Esta implementación está escrita en C, y la primera versión estable se liberó en 1998.

Fig. 5. Logo OpenLDAP.

Por otro lado, *Active Directory* es el servidor de directorio de Microsoft y necesitaremos un sistema Windows Server para poder instalarlo. En este enlace podrás ampliar la información sobre *Active Directory* directamente de la mano de Microsoft.

/ 4. Caso práctico 1: "Gestión de usuarios"

Planteamiento: Joaquín está desarrollando una aplicación web de contabilidad para una empresa y el cliente está interesado en utilizar un servidor de directorio para gestionar los inicios de sesión. Este cliente no contaba con un servidor de directorio, por lo que se le ha solicitado que facilite un listado de usuarios para realizar la importación al nuevo servidor LDAP, que el departamento de sistemas ha configurado. Tras recibir el listado, Joaquín se encuentra con más de 100 usuarios y teme que tenga que registrarlos uno a uno en el directorio.

Nudo: ¿Tendrá que importar todos los registros uno a uno? ¿Existe alguna manera rápida de añadir los usuarios al servidor de directorio?

Desenlace: Tras investigar un poco, Joaquín descubre que podrá utilizar los ficheros LDIF para realizar una carga masiva de usuarios en el servidor LDAP. A continuación, deberá adaptar el listado de usuarios a un fichero con extensión LDIF con la siguiente estructura:

```
dn: uid=maria,ou=sistemas,dc=directorio,dc=empresa,dc=com
objectClass: inetOrgPerson
uid: Maria
sn: Bonoso
cn: Maria Bonoso
givenName: maria
displayName: Maria Bonoso
```

Código 3. Ejemplo de un fichero LDIF para insertar datos.

Para finalizar, podrá realizar la importación en el servidor LDAP utilizando, por ejemplo, un gestor gráfico como podría ser **LDAP Admin.**

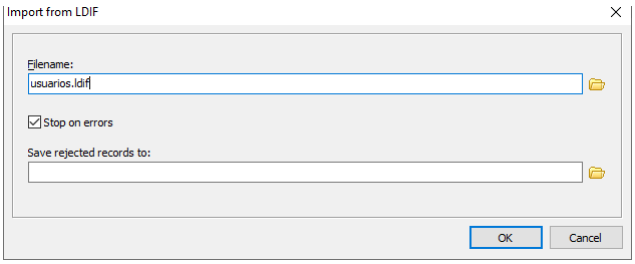

Fig. 6. LDAP Admin - Importar desde un archivo LDIF.

/ 5. Implementación del servicio OpenLDAP.

En este apartado se explicará de forma detallada cómo realizar la instalación de OpenLDAP en Ubuntu Server 18.04.

A modo de guía, los pasos que seguiremos serán los siguientes:

1. Instalación servicio SLAPD.
2. Configuración y puesta en marcha.
3. Creación de fichero LDIF y carga de datos.

Además, podríamos considerar un último paso, aunque no fuese propio de la instalación en sí misma, pero sí necesario para verificar la correcta importación de los registros utilizando **ldapsearch.**

a. **Instalación OpenLDAP**

Como para el resto de instalaciones, el primer paso será actualizar los repositorios de paquetes para, posteriormente, proceder a la instalación:

```
usuario@srv-openldap-01:~$ sudo apt-get install slapd ldap-utils
```

Código 4. Instalación LDAP en Ubuntu 18.04 – Pro Ubuntu Server Administration.

b. **Configuración de OpenLDAP**

Utilizaremos el comando **dpkg-reconfigure** para iniciar el asistente de configuración de **SLDAP** y definir el dominio que utilizaremos para nuestro directorio:

```
usuario@srv-openldap-01:~$ sudo dpkg-reconfigure slapd
  Backing up /etc/ldap/slapd.d in /var/backups/slapd-2.4.45+dfsg-1ubuntu1.6... done.
  Moving old database directory to /var/backups:
  - directory unknown... done.
Creating initial configuration... done.
Creating LDAP directory... done.
```

Código 5.Configuración LDAP en Ubuntu 18.04 – Pro Ubuntu Server Administration.

Una vez completemos el asistente de configuración, el sistema creará el fichero **ldap.conf** en la ruta **/etc/ldap.**

c. **Creación de fichero LDIF y carga de datos**

El siguiente paso será importar registros y comprobar que OpenLDAP funciona correctamente. Para ello, crearemos un fichero con el siguiente formato:

```
root@srv-openldap-01:~# nano import.ldif
dn: ou=contabilidad,dc=directorio,dc=empresa,dc=com
objectClass: organizationalUnit
ou: contabilidad

dn: ou=sistemas,dc=directorio,dc=empresa,dc=com
objectClass: organizationalUnit
ou: sistemas

dn: uid=javier,ou=contabilidad,dc=directorio,dc=empresa,dc=com
objectClass: inetOrgPerson
uid: javier
sn: Lopez
cn: Javier Lopez
givenName: javier
displayName: Javier Lopez

dn: uid=maria,ou=sistemas,dc=directorio,dc=empresa,dc=com
objectClass: inetOrgPerson
uid: Maria
sn: Bonoso
cn: Maria Bonoso
givenName: maria
displayName: Maria Bonoso
```

Código 6. Creación de fichero LDIF – Pro Ubuntu Server Administration.

A continuación, importamos los registros utilizando el siguiente comando:

```
slapadd -l import.ldif
```

Código 7. Utilizamos el comando slapadd para importar el fichero LDIF – Pro Ubuntu Server Administration.

5.1. Verificación de la importación de datos con ldapsearch

El comando **ldapsearch** nos permite realizar consultas al directorio. De esta manera, podremos comprobar que los registros se han importado correctamente o, simplemente, solicitar datos al servidor.

En el siguiente ejemplo, realizaremos una búsqueda en el dominio directorio.empresa.com:

```
root@srv-openldap-01:~# ldapsearch -x -b
“dc=directorio,dc=empresa,dc=com”
# extended LDIF
#
# LDAPv3
# base <dc=directorio,dc=empresa,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# directorio.empresa.com
dn: dc=directorio,dc=empresa,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: empresa
dc: directorio

. . .

# search result
search: 2
result: 0 Success

# numResponses: 7
# numEntries: 6
```

Código 8. Búsqueda en el directorio – Pro Ubuntu Server Administration.

El resultado del comando ejecutado en la imagen código 8 mostrará un listado completo de todos los registros del directorio.

Pero esto no es especialmente ágil, ya que a medida que el directorio crezca, será más complicado analizar el resultado de esta búsqueda.

Para facilitar la gestión, podemos utilizar filtros en las búsquedas y afinar los resultados utilizando modificadores como, por ejemplo, "uid". Este modificador mostrará los resultados que coincidan con el *uid* indicado:

```
root@srv-openldap-01:~# ldapsearch -x -b
"dc=directorio,dc=empresa,dc=com" uid=javier
# extended LDIF
#
# LDAPv3
# base <dc=directorio,dc=empresa,dc=com> with scope subtree
# filter: uid=javier
# requesting: ALL
#
# javier, contabilidad, directorio.empresa.com
dn: uid=javier,ou=contabilidad,dc=directorio,dc=empresa,dc=com
objectClass: inetOrgPerson
uid: javier
sn: Lopez
cn: Javier Lopez
givenName: javier
displayName:: SmF2aWVyIEzDs3Bleg==

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Código 9. Uso de LdapSearch filtrando el resultado – Pro Ubuntu Server Administration.

/ 6. Microsoft Active Directory

En lo que a servidores de directorio se refiere, ***Active Directory*** es un referente a nivel empresarial por su fácil administración y potencia. A diferencia de OpenLDAP, *Active Directory* cuenta con una interfaz de administración gráfica cómoda y sencilla de usar, aunque cabe destacar que utilizando **PowerShell,** podremos ejecutar consultas y realizar operaciones avanzadas introduciendo comandos.

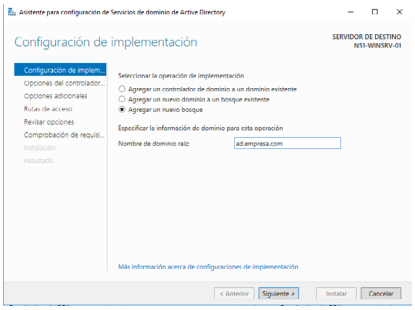

Fig. 7. Instalación de Active Directory en Windows Server.

La instalación se realizará utilizando el asistente para agregar roles y características. En el listado de roles disponibles, seleccionaremos **Servicios de dominio de *Active Directory*** y solo tendremos que avanzar en el asistente de instalación. Una vez concluya esta, deberemos promover el servidor a **controlador de dominio** utilizando el asistente.

En este asistente, definiremos el dominio DNS que utilizará el directorio.Asimismo, nos preguntará la operación de implementación, en la que elegiremos **Agregar un nuevo bosque** para crear una estructura nueva. Durante la instalación del servidor de dominio *Active Directory,* se instalará el servicio DNS.

Una vez termine el proceso de promoción a controlador de dominio, podremos gestionar los usuarios y grupos desde el **Administrador de usuarios y equipos de *Active Directory*.**

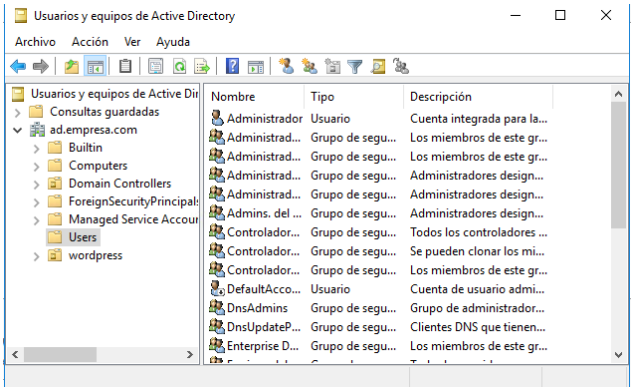

Fig. 8. Panel de administración de usuarios y equipos de Active Directory.

Audio 1. "Permitir tráfico LDAP"
https://bit.ly/39yBi5f

/ 7. Conexión LDAP con aplicación web

A la hora de desarrollar una aplicación web para una empresa, es posible que se establezca como requisito fundamental iniciar sesión utilizando los usuarios del servidor de directorio de dicha empresa.

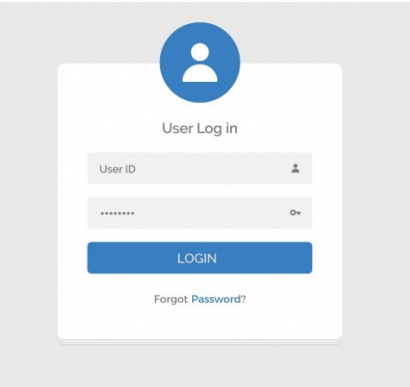

Fig. 9. El servicio de directorio permite que los usuarios inicien sesión en diferentes plataformas con una misma contraseña.

Esta característica, además de facilitar el acceso a los diferentes usuarios (pues podrán iniciar sesión con la misma contraseña que utilizan para acceder a su equipo), nos aportará seguridad y podremos configurar grupos personalizados para autorizar el login. Para autorizar el inicio de sesión a través de un servidor de directorio, necesitaremos conocer el **base DN,** es decir, el nombre de dominio en el que se realizará la búsqueda de usuarios. En este campo, podemos concretar una unidad organizativa o grupo para delimitar el acceso a los recursos.

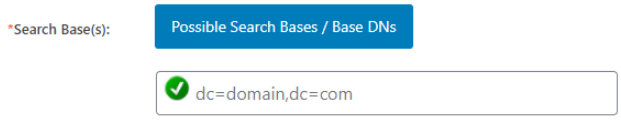

Fig. 10. Campo Base DN del módulo "LDAP/AD Login for Intranet" para Wordpress.

Además de conocer el Base DN del directorio, necesitaremos un usuario del propio directorio que autorice la conexión y realice las búsquedas de usuarios. Este proceso se conoce como **BIND** y consiste en un usuario intermedio que transmitirá las consultas de inicio de sesión al servidor LDAP y devolverá las respuestas a la aplicación, indicando si la combinación de usuario y contraseña coincide con la información almacenada en el servidor de directorio.

Vídeo 2. "LDAP utilizando aplicaciones en iniciar sesión"
https://bit.ly/3g1i6y4

/ 8. Caso práctico 2: "Limitar acceso por grupos en Wordpress"

Planteamiento: Myriam está configurando una aplicación web para un cliente y debe realizar la autenticación de usuarios a través del Directorio Activo de la empresa. Además, por motivos de calidad y seguridad, solo podrán iniciar sesión los usuarios pertenecientes al grupo "WebApp", que deberá crear en el AD.

Nudo: ¿Qué configuración deberá realizar en el Directorio Activo? ¿Cómo indicará a la aplicación qué grupo de usuarios deberá autorizar?

Desenlace: Para poder configurar el inicio de sesión utilizando usuarios del directorio de la empresa, Myriam deberá crear un nuevo grupo en el Active Directory de la compañía. Para ello, tendrá que abrir el administrador de usuarios y grupos de Active Directory y utilizar el asistente de creación de grupos. A continuación, deberá añadir los usuarios correspondientes a dicho grupo.

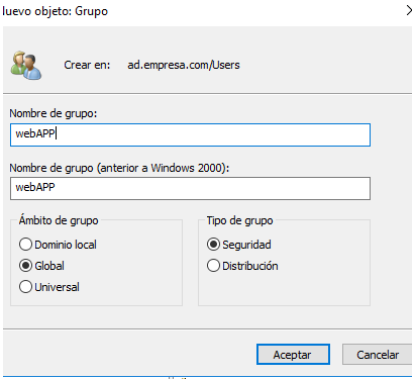

Fig. 11. Creación de un grupo en AD.

Lo siguiente que debe hacer es configurar la aplicación web para que utilice usuarios del grupo correcto. Esta configuración se realizará indicando a la aplicación el grupo en la **base DN:**

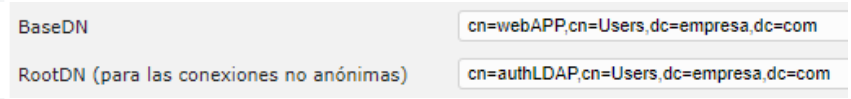

Fig. 12. Configuración BaseDN en aplicación web.

/ 9. Resumen y resolución del caso práctico de la unidad

En esta unidad, hemos aprendido que los **servidores de directorio** son una pieza fundamental en entornos empresariales donde se requiere un **control de usuarios y grupos.**

En el marco práctico, hemos aprendido a **instalar y configurar** servidores de directorio y a sincronizar el inicio de sesión de una aplicación web.

De esta manera, queda clara la importancia que tiene el servicio.

Fig. 13. El servicio de directorio como sistema de autenticación centralizado.

Resolución del caso práctico inicial

En el caso práctico inicial, se planteó la siguiente situación: en el proceso de modernización digital, una empresa va a invertir en aplicaciones web y quiere implementar un sistema de inicio de sesión polivalente.

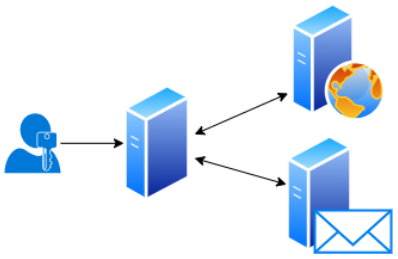

Fig. 14. Single Sign On.

La solución más acertada sería basar todos los servicios en autenticación LDAP.

Para ello, necesitarán, al menos, un servidor de directorio que gestione los usuarios de la empresa.

A partir de ahí, podrán seguir ampliando servicios que permitan autenticación LDAP, como podrían ser servidores de correo, aplicaciones webs, inicio de sesión en los equipos de la empresa, etc.

/ 10. Bibliografía

Mesa, V. J.M. (s. f.). *Desarrollo web en entorno servidor* (Grado superior). RA-MA S.A. Editorial y Publicaciones.

Redbooks, I. (2004). Understanding Ldap - Design And Implementation. -, -: IBM.

/ 11. Webgrafía

https://docs.oracle.com/cd/E10773_01/doc/oim.1014/e10531/ldif_appendix.htm

https://www.rediris.es/ldap/doc/ldap-intro.pdf

https://www.openldap.org/doc/admin24/

https://es.wordpress.org/plugins/ldap-login-for-intranet-sites/