Tema 9

Administración de servicios de directorio

Administración de Sistemas Operativos

Índice

[Esquema 3](#_Toc170825856)

[Material de estudio 4](#_Toc170825857)

[9.1. Introducción y objetivos 4](#_Toc170825858)

[9.2. Servicios de directorio LDAP 4](#_Toc170825859)

[9.3. Instalación, configuración y personalización del servicio de directorio. OpenLDAP. 6](#_Toc170825860)

[9.4. Directorios. Administración y operaciones. Dominios. 18](#_Toc170825861)

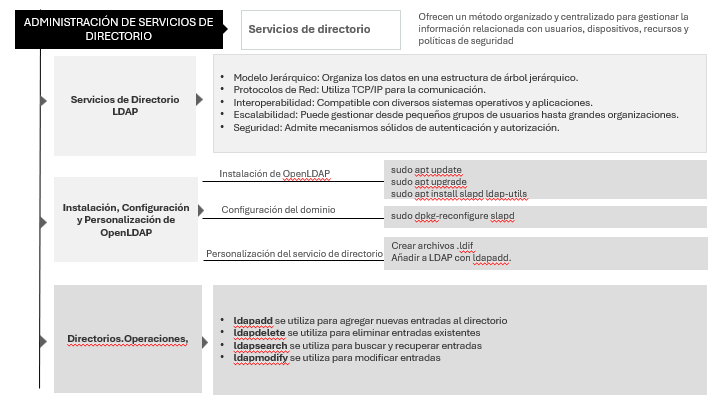
[9.5. Referencias bibliográficas 22](#_Toc170825862)

[A fondo 24](#_Toc170825863)

[Entrenamientos 25](#_Toc170825864)

[Test 29](#_Toc170825865)

Esquema



Material de estudio

9.1. Introducción y objetivos

Los servicios de directorio son esenciales en la gestión de sistemas informáticos, ya que ofrecen una forma organizada y centralizada de manejar información sobre usuarios, dispositivos, recursos y políticas de seguridad. Estos servicios permiten a los administradores de sistemas regular el acceso a los recursos en una red y gestionar cómo se utilizan dichos recursos.

Los objetivos que se pretenden alcanzar en este tema son :

* **Adquirir una comprensión básica** de los servicios de directorio y su importancia en la administración de sistemas.
* **Familiarizarse con el protocolo LDAP** y comprender su funcionamiento.
* **Realizar la instalación, configuración y personalización** de un servicio de directorio utilizando OpenLDAP.
* **Gestionar y operar directorios y dominios,** incluyendo la administración de usuarios, grupos y políticas.
* **Aplicar prácticas recomendadas de seguridad** y garantizar la integridad de la información en el contexto de los servicios de directorio…

9.2. Servicios de directorio LDAP

LDAP (Lightweight Directory Access Protocol), o Protocolo Ligero de Acceso a Directorios, es un conjunto de protocolos, de la capa de aplicación, multiplataforma de código abierto utilizado para acceder y mantener servicios de directorio distribuidos a través de una red. Proporciona un método eficiente y estructurado para almacenar y recuperar datos. LDAP es ampliamente utilizado debido a su compatibilidad con diferentes sistemas operativos y aplicaciones, así como por su capacidad para manejar grandes volúmenes de información.

Un servicio de directorio es una base de datos centralizada que almacena información sobre usuarios, grupos, dispositivos y otros recursos de red. LDAP es comúnmente utilizado para este tipo de servicios.

El funcionamiento de LDAP se basa en un modelo cliente-servidor. Un servidor LDAP almacena la información del directorio y un cliente LDAP, como una aplicación o servicio de usuario, se conecta al servidor para realizar consultas o modificaciones

Algunas características clave de LDAP son:

* Modelo Jerárquico: LDAP organiza los datos en una estructura de árbol jerárquico, similar a un sistema de archivos. Cada nodo representa una entrada (por ejemplo, un usuario o un grupo) con atributos.
* Protocolos de Red: Utiliza TCP/IP para la comunicación, lo que facilita su integración en redes existentes.
* Interoperabilidad: Es compatible con diversos sistemas operativos y aplicaciones, lo que permite su adopción en entornos heterogéneos.
* Escalabilidad: LDAP tiene la capacidad de gestionar desde pequeños grupos de usuarios hasta grandes organizaciones con millones de entradas.
* Seguridad: LDAP admite mecanismos sólidos de autenticación y autorización, así como la encriptación de datos durante la transmisión.

LDAP tiene unas desventajas que es necesario considerar a la hora de su utilización:

* Complejidad: Puede ser complejo de configurar y administrar.
* Rendimiento: En entornos con un gran volumen de escrituras, puede ser menos eficiente que otras bases de datos.

En conclusión, LDAP es una herramienta poderosa para la gestión de directorios de servicios y es crucial para cualquier profesional de TI que trabaje con redes y sistemas de información.

En el apartado A Fondo puedes encontrar un vídeo introductorio sobre LDAP.

9.3. Instalación, configuración y personalización del servicio de directorio. OpenLDAP.

El protocolo LDAP se basa en un modelo cliente-servidor que permite interactuar con un directorio jerárquico de información. Este directorio está diseñado para ser eficiente en la recuperación y consulta de datos, funcionando de manera similar a una base de datos, pero con una mayor rapidez en la realización de búsquedas y lecturas. Por otro lado, OpenLDAP se destaca como una solución ampliamente reconocida y adaptable para la creación de directorios LDAP, gracias a su condición de software libre y de código abierto, lo cual facilita su uso y personalización sin costo alguno.

OpenLDAP ofrece la posibilidad de:

* **Verificar la identidad de los usuarios** en distintos sistemas distribuidos por una red.
* **Consolidar la administración de usuarios y grupos**, facilitando así la gestión de derechos y accesos.
* **Realizar búsquedas y recuperar datos de forma eficaz** gracias a su estructura jerárquica.
* Representa una opción perfecta para aquellas organizaciones que desean una **manera normalizada y efectiva de administrar volúmenes** significativos de información de directorio, con un enfoque particular en la seguridad y la autenticación. OpenLDAP es una herramienta utilizada en sectores corporativos, educativos y gubernamentales, y ofrece compatibilidad con un amplio espectro de aplicaciones y servicios.

En este capítulo vamos a realizar la instalación de OpenLDAP sobre el sistema operativo Ubuntu Server.

9.3.1. Instalación de OpenLDAP

Para instalar OpenLDAP, necesitarás seguir estos pasos generales:

1. En primer lugar, hay que asegurarse que el sistema esté actualizado con los últimos paquetes. Para ello usaremos:

Texto

Descripción generada automáticamente

Figura 1. Comandos para actualización de paquetes. Fuente: elaboración propia.

para actualizar la lista de paquetes y versiones. Una vez finalizada la instalación de paquete usaremos el comando para actualizar los paquetes a las últimas versiones disponibles.



Figura 2. Comandos para asegurar últimas versiones de paquetes. Fuente: elaboración propia.

1. A continuación, instalamos slapd y ldap-utils, que son esenciales para OpenLDAP.



Figura 3. Comandos para instalar OpenLdap. Fuente: elaboración propia.

Durante la instalación, se solicita que se configure el dominio y la contraseña del administrador de LDAP (rootDN). Esta contraseña va a ser utilizada posteriormente.

Interfaz de usuario gráfica, Texto, Aplicación, Teams

Descripción generada automáticamente

Figura 4. Instalación de OpenLdap, contraseña de administrador. Fuente: elaboración propia.

Después de la instalación, es necesario proceder con la configuración y personalización de OpenLDAP. Los pasos recomendados son:

* Definir el FQDN: Asignar el Nombre de Dominio Totalmente Cualificado del servidor para asegurar una correcta resolución de nombres.
* Personalizar la configuración: Si fuera necesario, ajustar el archivo slapd.conf para que refleje las necesidades específicas del entorno.
* Incorporar datos al directorio: Emplear archivos LDIF para introducir nuevas organizaciones, usuarios y grupos en el directorio LDAP.

9.3.2. Configuración de OpenLDAP

A continuación, se detallan los pasos a seguir para configurar OpenLDAP según las características de nuestra organización:

1. Utilizamos dpkg-reconfigure en Debian/Ubuntu para reconfigurar el dominio del servidor LDAP:



Figura 5. Reconfiguración de OpenLdap. Fuente: elaboración propia.

En la siguiente ventana indicamos que no queremos omitir la configuración de paquetes poque queremos realizarla. En este paso se va a proceder a realizar una base de datos y una configuración iniciales de OpenLDAP.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 6. Reconfiguración de OpenLdap, configuración de la base de datos. Fuente: elaboración propia.

A continuación, aparece una ventana donde indicaremos el dominio que queremos utilizar. Este dominio será el que nos indiquen desde la empresa. En nuestro caso vamos a crear un dominio genérico llamado “midominio.com” con el que trabajaremos el resto de los pasos.



Figura 7. Reconfiguración de OpenLdap, alta del dominio Fuente: elaboración propia.

Posteriormente nos indica cual es el nombre de la organización, por defecto pondremos el mismo que hemos usado como nombre de dominio.

Texto

Descripción generada automáticamente

Figura 8. Reconfiguración de OpenLdap, alta de la organización. Fuente: elaboración propia.

En este punto crearemos la contraseña que va a utilizar el administrador de LDAP. Nos pedirá confirmación de la contraseña.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 9. Reconfiguración de OpenLdap, contraseña del administrador. Fuente: elaboración propia.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 10. Reconfiguración de OpenLdap, contraseña del administrador. Fuente: elaboración propia.

Borramos la base de datos anterior ya que genera una por defecto con la instalación de slapd y no la necesitamos.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 11. Reconfiguración de OpenLdap, borrado de la base de datos. Fuente: elaboración propia.

Le indicamos que mueva los ficheros relacionados con bases de datos antiguas. Estos ficheros ya no son necesarios porque vamos a crear nuestra propia base de datos nueva.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 12. Reconfiguración de OpenLdap, mover ficheros de la base de datos antigua. Fuente: elaboración propia.

Una vez finalizada la instalación, si todo ha ido bien, nos debe mostrar el siguiente mensaje que finaliza indicando que ha creado LDAP Directory.

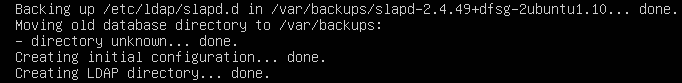


Figura 13. Mensaje de salida de configuración OpenLdap. Fuente: elaboración propia.

Hemos completado con éxito la configuración del LDAP bajo nuestro propio dominio. Para confirmar que la implementación se ha realizado correctamente, te invito a emplear el comando `**slapcat**`, el cual revelará los detalles pertinentes de nuestro dominio LDAP. Observarás que el dominio establecido es **midominio.com**, y contamos con un usuario denominado **admin**, quien ostentará las funciones de administrador de nuestro sistema LDAP.

Texto

Descripción generada automáticamente

Figura 14. Salida del comando slapcat. Fuente: elaboración propia.

Con la configuración actualmente establecida, estamos en disposición de comenzar a incorporar objetos a nuestro dominio. Procederemos a la creación de una organización, un grupo y un usuario, demostrando así el proceso a seguir. Es posible ampliar la estructura con la adición de usuarios y grupos adicionales, adaptándose a los requerimientos específicos de la empresa o del proyecto en curso.

9.3.3. Personalización del Servicio

En este apartado realizaremos una jerarquía de directorio en forma de árbol que represente la estructura de la organización.

LDAP tiene una estructura jerárquica según el siguiente árbol:

Diagrama

Descripción generada automáticamente

Figura 15. Árbol de directorios LDAP. Fuente: https://somebooks.es/capitulo-11-instalar-y-configurar-openldap-en-ubuntu-14-04-lts/2/

Para llevar a cabo esta tarea, procederemos a elaborar archivos **LDIF** en los cuales incorporaremos la información necesaria antes de su integración en el servidor. Estos archivos serán creados dentro de nuestro directorio **home**. Un archivo LDIF detalla la estructura estándar de datos para el registro de organizaciones, grupos y usuarios en LDAP, incluyendo los atributos fundamentales y la configuración acorde con los esquemas y las políticas de seguridad inherentes al sistema.

Aunque es factible consolidar toda la estructura organizativa en un único archivo LDIF que englobe la unidad organizativa, los grupos y los usuarios para su carga simultánea, esta metodología incrementa el riesgo de errores. Por ello, optaremos por generar un archivo distinto para cada elemento de la jerarquía, garantizando así una mayor precisión y estabilidad en el proceso de configuración.

Hay que tener en cuenta que el orden es muy importante a la hora de crear la jerarquía, estableciéndose primero la Unidad organizativa, posteriormente el grupo y por último los usuarios.

El primer paso consistirá en establecer una **Unidad Organizativa (OU)**, que nos permitirá clasificar de manera eficiente usuarios, grupos y otros componentes. Para ello, generaremos un archivo denominado `ou.ldif`. Este archivo lo editaremos utilizando el comando `nano`, facilitando así la introducción y organización de los datos requeridos.



Figura 16. Creación del fichero ou.dif. Fuente: Elaboración propia.

Y cuyo contenido será el siguiente

Forma, Rectángulo

Descripción generada automáticamente

Figura 17. Contenido del fichero ou.dif. Fuente: Elaboración propia.

dn: ou=asir,dc=midominio,dc=com -> la unidad organizativa se llamar asir

objectClass: top -> indica que cuelga directamente de la raiz

objectClass: organizationalUnit -> indica que es una unidad organizativa

ou: asir -> nombre de la unidad organizativa

Los atributos **objectClass** definen las características y propiedades del objeto en el directorio LDAP. Cada clase de objeto (posixGroup, inetOrgPerson, person) define conjuntos específicos de atributos que pueden ser utilizados para ese objeto en particular. Por ejemplo, posixGroup proporciona atributos relacionados con los grupos, como el número de identificación.

Las opciones top, posixAccount, inetOrgPerson, person son posibles en objetcClass. Top indica que es la clase superior para todas las entradas LDAP, posixAccount indica que este objeto representa una cuenta POSIX, lo que implica que tiene atributos como uidNumber, gidNumber, homeDirectory, y loginShell, inetOrgPerson especifica que este objeto es un elemento según el esquema de LDAP de tipo "Internet Organization" y person especifica que este objeto es una persona genérica.

El siguiente paso es importar el archivo ou.ldif que acabamos de crear al sistema LDAP. Para ello, utilizaremos el comando **ldapadd**, que nos permitirá agregar la nueva entrada a la base de datos.

Texto

Descripción generada automáticamente

Figura 18. Incorporación de la unidad organizativa a ldap. Fuente: elaboración propia.

Este comando solicitará la contraseña del administrador LDAP y, tras su introducción, procederá a cargar la información contenida en el archivo ou.ldif al servidor LDAP. Es importante asegurarse de que la ruta al archivo y los detalles de conexión sean correctos para evitar errores en el proceso.

Continuaremos con la creación de un grupo dentro de la Unidad Organizativa previamente establecida. Comenzaremos abriendo el terminal y ejecutando el comando nano grupos.ldif para crear y editar el archivo correspondiente al grupo. Una vez dentro del editor nano se procede a añadir el siguiente contenido:Texto

Descripción generada automáticamente

Figura 19. Contenido del fichero grupos.ldif. Fuente: elaboración propia.

Donde “segundo” es el nombre que le hemos dado al grupo dentro de la unidad organizativa asir. El idNumber es el número de identificador que se le da al grupo, se recomienda que los identificadores que se necesiten en ldap empiecen en 2000 ya que los anteriores a este número se usan para usuarios y grupos locales.

A continuación, integraremos el nuevo grupo al sistema LDAP utilizando el mismo procedimiento que en la operación anterior. La diferencia radica en especificar el archivo del grupo recién creado. Una vez ejecutado el comando con éxito, se nos presentará un mensaje confirmando que la nueva entrada ha sido añadida satisfactoriamente. Aquí tienes un ejemplo de cómo es el comando que se debe utilizar

ldapadd -x -D cn=admin,dc=midomiono,dc=com -W -f grupos.ldif

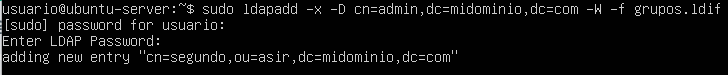


Figura 20. Incorporación de grupos a ldap. Fuente: elaboración propia.

Este proceso añadirá el grupo al directorio LDAP, y si todo transcurre sin inconvenientes, recibirás una confirmación en la terminal que indica la correcta adición de la entrada.

Finalmente, para incorporar un usuario al grupo recién creado, replicaremos el procedimiento previo, con la diferencia de que ahora generaremos un archivo denominado usuarios.ldif dedicado exclusivamente a este usuario. Dentro de este archivo, asignaremos al usuario una contraseña encriptada, la cual crearemos de antemano para posteriormente integrarla.

La creación de la contraseña encriptada se realizará mediante el comando **slappasswd**, que nos proporcionará una contraseña segura y encriptada utilizando el protocolo SSHA (Salted Secure Hash Algorithm) adecuada para el uso del usuario en el sistema LDAP. Aquí tienes un ejemplo de cómo generar la contraseña:

Texto

Descripción generada automáticamente

Figura 21. Creación de contraseña encriptada. Fuente: elaboración propia.

Tras ejecutar el comando, copia la contraseña encriptada resultante y la incluyes en el archivo usuarios.ldif para completar la configuración del usuario.

Ahora procedemos a crear el fichero usuarios.ldif con el contenido siguiente y usando la contraseña generada en el punto anterior:

dn: uid=nuevoUsuario,ou=asir,dc=midominio,dc=com

objectClass: top

objectClass: posixAccount

objectClass: inetOrgPerson

objectClass:person

cn: nuevoUsuario

uid: nuevoUsuario

uidNumber: 2000

gidNumber: 2000

homeDirectory: /home/nuevoUsuario

loginShell: /bin/bash

userPassword: {SSHA} 6Y6Vw+1drf61+DgLYscMV05P29RrASGy

sn: nuevoUsuario

mail: [nuevoUsuario@midominio.com](mailto:nuevoUsuario@midominio.com)

givenName: nuevoUsuario

Texto

Descripción generada automáticamente

Figura 22. Creación de fichero de usuarios. Fuente: elaboración propia.

Veamos cada uno de los atributos indicados:

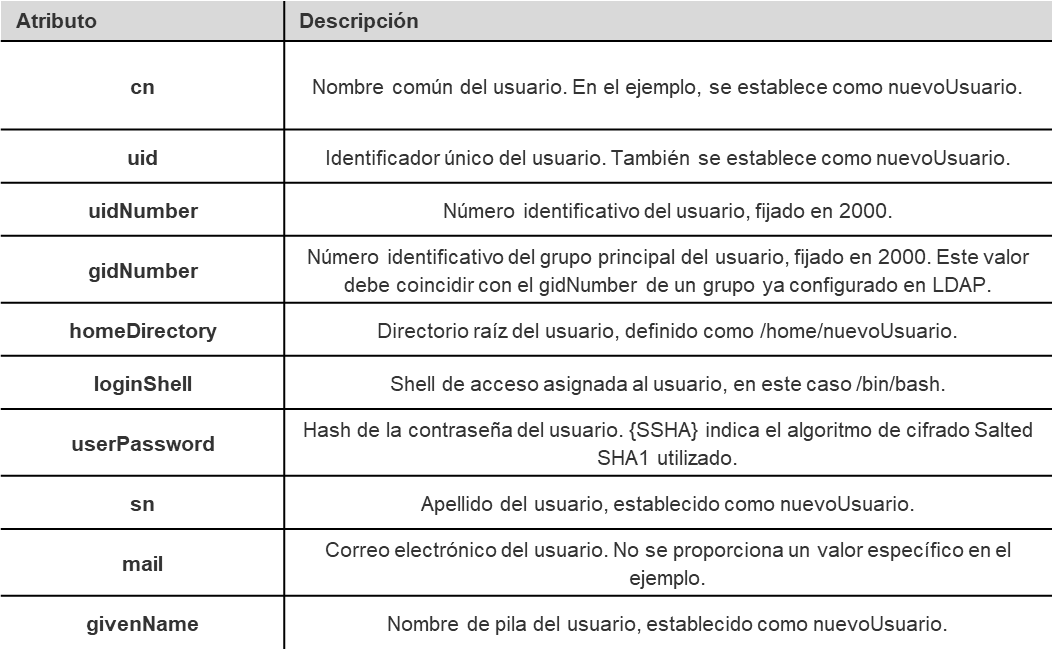


Tabla 1. Significado de los atributos de un usuario. Fuente: elaboración propia.

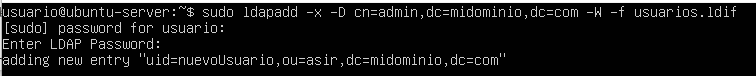
Para concluir el proceso, añadiremos la entrada del usuario al sistema LDAP siguiendo el mismo método empleado para la organización y el grupo. Aquí tienes un ejemplo del comando que realizará esta acción:

Figura 23. Incorporación de usuarios a ldap. Fuente: elaboración propia.

Este comando solicita la contraseña del administrador LDAP. Una vez proporcionada, el sistema procesará el archivo usuarios.ldif y añadirá la entrada del usuario al directorio LDAP.

Con estos pasos, se ha completado satisfactoriamente la configuración de tu estructura LDAP. Para comprobar que las actualizaciones se han realizado correctamente, el comando **slapcat** devuelve los detalles de la jerarquía realizada.

En el apartado A Fondo puedes encontrar un vídeo explicativo de cómo instalar y configurar OpenLdap en un servidor Ubuntu y en cliente.

9.4. Directorios. Administración y operaciones. Dominios.

9.4.1. Directorios. Administracion y operaciones.

La información en OpenLDAP se estructura en un árbol jerárquico conocido como DIT (Directory Information Tree).

Diagrama

Descripción generada automáticamente con confianza baja

Figura 24. Estructura de árbol jerárquico en ldap. Fuente: Elaboración propia.

Las entradas se generan usando los ficheros LDIF como hemos visto anteriormente y mediante los siguientes comandos:

* **ldapadd** se utiliza para agregar nuevas entradas al directorio LDAP.

ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f archivo.ldif

En este contexto, la opción -x señala la utilización de una autenticación simple, mientras que -D designa al usuario administrador. Por su parte, -W invita a introducir la contraseña del administrador, y -f determina el archivo LDIF que alberga las entradas que serán incorporadas. El contenido de archivo.ldif es el siguiente y se utiliza para crear un usuario llamado jdoe.

dn: uid= jdoe,ou=people,dc=example,dc=com

objectClass: inetOrgPerson

objectClass: person

uid: jdoe

cn: John Doe

sn: Doe

mail: jdoe@example.com

userPassword: secret

* **ldapdelete** se utiliza para eliminar entradas existentes en el directorio LDAP. En este caso estamos borrando el usuario creado anteriormente.

ldapdelete -x -D "cn=admin,dc=example,dc=com" -W "uid=jdoe,ou=people,dc=example,dc=com"

* **ldapsearch** se utiliza para buscar y recuperar entradas del directorio LDAP. En este ejemplo estamos buscando dentro de LDAP las entradas que contienen uid=joe

ldapsearch -x -b "ou=people,dc=example,dc=com" "(uid=jdoe)"

* **ldapmodify** se utiliza para modificar entradas existentes en el directorio LDAP.

ldapmodify -x -D "cn=admin,dc=example,dc=com" -W -f archivo\_modificaciones.ldif

Donde el fichero de modificación sería el siguiente:

dn: uid=jdoe,ou=people,dc=example,dc=com

changetype: modify

replace: mail

mail: john.doe@example.com

Y los tipos de modificaciones posibles:

* Agregar Atributos: changetype: add
* Reemplazar Atributos: changetype: modify
* Eliminar Atributos: changetype: delete

9.4.2. Dominios.

En el contexto de LDAP y Ubuntu Server, un dominio es una unidad administrativa que agrupa recursos de red, usuarios y computadoras. En la práctica, esto se traduce en un espacio de nombres LDAP. Cada dominio tiene su propia base de datos y políticas de seguridad.

Como hemos visto en el apartado anterior, la estructura de un dominio LDAP en Ubuntu Server se organiza jerárquicamente, utilizando unidades organizativas (OU) para agrupar objetos. Llegado a este punto, tenemos creado un dominio llamado “midominio.com” al que hemos añadido un grupo y un usuario.

En LDAP se permite la creación de **subdominios** dentro de un dominio previamente creado. Un subdominio en el contexto de LDAP es una subdivisión dentro de un dominio principal que se estructura de forma jerárquica. Aunque forma parte del dominio principal, puede gestionarse de manera semi-independiente.

Se representa mediante la adición de un nuevo componente de dominio (dc) al principio del nombre distinguido (DN) del dominio principal. Por ejemplo, si el dominio principal es `dc=midominio,dc=com`, un subdominio podría ser `dc=ventas,dc=midominio,dc=com`.

Permite organizar y segmentar la información dentro del directorio y facilita la administración de grandes cantidades de datos o estructuras organizativas complejas. Se pueden crear múltiples niveles de subdominios según sea necesario.

Un subdominio puede tener sus propias políticas y configuraciones y sus propias unidades organizativas (OU), usuarios, grupos, etc.

Supongamos que queremos diseñar la siguiente estructura para el dominio “midominio.com” :

* Dominio raíz: midominio.com
* Subdominio: ventas. midominio.com

Pasos para implementarlo:

1. En el servidor LDAP del dominio raíz, se añade una referencia al subdominio. Se crea un fichero llamado add\_ventas.ldif cuyo contenido es el siguiente:

dn: dc=ventas,dc=midominio,dc=com

objectClass: top

objectClass: domain

dc: ventas

dn: ou=users,dc=ventas,dc=midominio,dc=com

objectClass: organizationalUnit

ou: users

dn: ou=groups,dc=ventas,dc=midominio,dc=com

objectClass: organizationalUnit

ou: groups

Texto

Descripción generada automáticamente

Figura 25.Contenido del fichero add\_ventas. Fuente: Elaboración propia.

Y añadimos la entrada a ldap

Texto

Descripción generada automáticamente

Figura 26. Incorporación de subdominio ventas. Fuente: Elaboración propia.

Para verificar que se ha realizado correctamente usaremos:

ldapsearch -x -LLL -b "dc=midominio,dc=com" "(objectClass=\*)"

Este comando ldapsearch realiza una búsqueda completa en el directorio LDAP, buscando en todo el dominio "midominio.com", recuperando todas las entradas (debido a "(objectClass=\*)") y mostrando los resultados en formato conciso (-LLL).

Estos pasos permiten crear y gestionar dominios y subdominios LDAP en Ubuntu Server, proporcionando una base sólida para la administración de sistemas distribuidos en entornos empresariales.

9.5. Referencias bibliográficas

LDAP.com. (s.f.). *LDAP.com.* https://ldap.com/

Red Hat. (3 de julio de 2022). *¿Qué es la autenticación LDAP?* <https://www.redhat.com/es/topics/security/what-is-ldap-authentication>

De Luz, S. (23 de mayo de 2024 ). *Para qué sirve el protocolo LDAP y cómo funciona.* RedesZone. <https://www.redeszone.net/tutoriales/servidores/que-es-ldap-funcionamiento/>

Ruiz, P. (3 de enero de 2015). *Capítulo 12: Instalar y configurar OpenLDAP en Ubuntu.* SomeBooks. https://somebooks.es/capitulo-11-instalar-y-configurar-openldap-en-ubuntu-14-04-lts/2/

A fondo

**Introducción a LDAP**

Linux al Sur. (21 de septiembre de 2023).  *Introducción al protocolo LDAP.* [Vídeo]. Youtube. https://www.youtube.com/watch?v=ONb3XmplCVY

Breve introducción a LDAP, arquitectura, características, seguridad e implementaciones.

**Instalar y configurar OpenLDAP**

Clockwork Computer. (31 de enero de 2023). *Instalar y configurar OpenLDAP en SERVIDOR y CLIENTE en Ubuntu Server & Desktop 22.04* [Vídeo]. Youtube. https://www.youtube.com/watch?v=Rl032gHFu88

El video muestra cómo instalar y configurar OpenLDAP en Ubuntu Server y Desktop 22.04, explicando los pasos necesarios tanto en el servidor como en el cliente.

Entrenamientos

**Entrenamiento 1**

* **Planteamiento del ejercicio**: Instalar y configurar OpenLDAP en un servidor Ubuntu.
* **Desarrollo paso a paso**:

1. Actualizar la lista de paquetes y versiones.
2. Instalar slapd y ldap-utils.
3. Configurar el dominio “aso.com” y la contraseña del administrador LDAP.

* **Solución**:

Actualizar la lista de paquetes y versiones.

sudo apt update

sudo apt upgrade

Instalar slapd y ldap-utils.

sudo apt install slapd ldap-utils

Configurar el dominio “aso.com” y la contraseña del administrador LDAP.

sudo dpkg-reconfigure slapd

**Entrenamiento 2**

* **Planteamiento del ejercicio**: Crear una Unidad Organizativa (OU) en LDAP llamada “administracion” en el dominio “aso” creado en el punto anterior.
* **Desarrollo paso a paso**:

1. Crear un archivo ou.ldif con la estructura de la OU.
2. Utilizar el comando ldapadd para agregar la OU al directorio LDAP.
3. Verifica que los cambios son correctos

* **Solución**:

Crear un archivo ou.ldif con la estructura de la OU.

nano ou.ldif

Contenido de ou.ldif ( Guardar el archivo con ctrl+O y Crtl+X para salir)

dn: ou=administracion,dc=aso,dc=com

objectClass: organizationalUnit

ou: administracion

Utilizar el comando ldapadd para agregar la OU al directorio LDAP.

sudo ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f ou.ldif

Para verificarlo

ldapsearch -x -LLL -b "dc=aso,dc=com" "ou=administracion"

**Entrenamiento 3**

* **Planteamiento del ejercicio**: Añadir un grupo llamado “directivos” a la Unidad Organizativa “administracion” creada en el apartado anterior en LDAP.
* **Desarrollo paso a paso**:

1. Crear un archivo grupos.ldif con la información del grupo.
2. Utilizar el comando ldapadd para agregar el grupo al directorio LDAP.
3. Verifica que los cambios son correctos

* **Solución**:

Crear un archivo grupos.ldif con la información del grupo.

nano grupos.ldif

Contenido de grupos.ldif ( Guardar el archivo con ctrl+O y Crtl+X para salir)

dn: cn=directivos,ou=administracion,dc=aso,dc=com

objectClass: top

objectClass: posixGroup

cn: directivos

gidNumber: 5000

Utilizar el comando ldapadd para agregar el grupo al directorio LDAP.

sudo ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f grupos.ldif

Para verificarlo

ldapsearch -x -LLL -b "ou=administracion,dc=example,dc=com" "cn=directivos"

**Entrenamiento 4**

* **Planteamiento del ejercicio**: Incorporar un usuario a un grupo en LDAP. Añade un usuario “Maria” al grupo “directivos” de la unidad “administracion”
* **Desarrollo paso a paso**:

1. Crear una contraseña encriptada usando slappasswd.
2. Crear un archivo usuarios.ldif con la información del usuario.
3. Utilizar el comando ldapadd para agregar el usuario al directorio LDAP.

* **Solución**:

Crear una contraseña encriptada usando slappasswd.

slappasswd

Crear un archivo usuarios.ldif con la información del usuario.

nano usuarios.ldif

Contenido de usuarios.ldif con la contraseña generada( Guardar el archivo con ctrl+O y Crtl+X para salir)

dn: uid=maria,ou=administracion,dc=aso,dc=com

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: top

cn: Maria

sn: User

uid: maria

uidNumber: 1001

gidNumber: 5000

homeDirectory: /home/maria

loginShell: /bin/bash

userPassword: {SSHA}5ENcrZCyRmWAGqY1E8y4KNleG7+Yb87y – esta es la contraseña generada con slappasswd

Utilizar el comando ldapadd para agregar el usuario al directorio LDAP.

sudo ldapadd -x -D "cn=admin,dc=aso,dc=com" -W -f usuarios.ldif

Crea el archivo add\_to\_group.ldif donde vamos a indicar al nuevo usuario el grupo al que pertenece:

dn: cn=directivos,ou=administracion,dc=aso,dc=com

changetype: modify

add: memberUid

memberUid: maria

Utilizar el comando ldapmodify para actualizar el usuario en el grupo

sudo ldapmodify -x -D "cn=admin,dc=aso,dc=com" -W -f add\_to\_group.ldif

**Entrenamiento 5**

* **Planteamiento del ejercicio**: Crear un subdominio “entrega” dentro de “aso” en LDAP.
* **Desarrollo paso a paso**:

1. Crear un archivo add\_entrega.ldif con la estructura del subdominio.
2. Utilizar el comando ldapadd para agregar el subdominio al directorio LDAP.
3. Verifica que los cambios se han realizado correctamente

* **Solución**:

Contenido de add\_entrega.ldif con la contraseña generada(Guardar el archivo con ctrl+O y Crtl+X para salir)

dn: dc=entrega,dc=aso,dc=com

objectClass: top

objectClass: domain

dc: entrega

Utilizar el comando ldapadd para agregar el subdominio al directorio LDAP.

sudo ldapadd -x -D "cn=admin,dc=aso,dc=com" -W -f add\_entrega.ldif

Verificación

ldapsearch -x -LLL -b "dc=entrega,dc=aso,dc=com"

Test

1. ¿Qué significa LDAP?

A. Large Directory Access Protocol

B. Lightweight Database Access Protocol

\_ C. Lightweight Directory Access Protocol

D. Local Directory Authentication Protocol

La opción C es correcta. LDAP significa Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios). Las demás alternativas no son válidas debido a que incluyen términos ajenos a las siglas LDAP o porque no representan su significado real.

2. ¿Cuál es una característica clave de LDAP?

A. Utiliza SQL para consultas

B. Solo funciona en sistemas Windows

\_ C. Organiza los datos en una estructura de árbol jerárquico

D. Requiere una conexión a Internet constante

La opción C es correcta. LDAP organiza los datos en una estructura de árbol jerárquico, similar a un sistema de archivos. Las otras opciones son incorrectas: LDAP no utiliza SQL, es multiplataforma y no requiere una conexión a Internet constante para funcionar.

3. ¿Qué comando se utiliza para instalar OpenLDAP en Ubuntu?

A. apt-get install ldap

B. yum install openldap

C. install openldap

\_D. apt-get install slapd ldap-utils

La opción D es correcta. El comando para instalar OpenLDAP en Ubuntu es "apt-get install slapd ldap-utils". La respuesta apt-get install ldap no es correcta, ya que "ldap" no es un paquete en Ubuntu, sino más bien un protocolo. La respuesta B. yum install openldap tampoco es correcta, ya que yum es el gestor de paquetes de sistemas basados en Red Hat, mientras que Ubuntu utiliza apt-get. En el caso de C. install openldap - tampoco es correcto, ya que falta el prefijo apt-get para indicar al sistema que instale el paquete a través del gestor de paquetes de Ubuntu.

4. ¿Qué significa FQDN en el contexto de LDAP?

A. Full Query Domain Name

\_ B. Fully Qualified Domain Name

C. Frequent Query Domain Network

D. Fast Query Directory Name

La opción B es correcta. FQDN significa Fully Qualified Domain Name (Nombre de Dominio Completamente Calificado). Las otras opciones son incorrectas ya que no representan el significado correcto de FQDN en el contexto de LDAP.

5. ¿Qué comando se utiliza para reconfigurar el dominio del servidor LDAP en Debian/Ubuntu?

A. ldapconfig

B. slapd-config

\_ C. dpkg-reconfigure slapd

D. ldap-domain-setup

La opción C es correcta. El comando "dpkg-reconfigure slapd" se utiliza para reconfigurar el dominio del servidor LDAP en Debian/Ubuntu. El resto de las opciones no son comandos válidos para esta tarea.

6. ¿Qué extensión tienen los archivos que se utilizan para añadir información al directorio LDAP?

A. .ldap

\_ B. .ldif

C. .conf

D. .dir

La opción B es correcta. Los archivos con extensión .ldif (LDAP Data Interchange Format) se utilizan para añadir información al directorio LDAP. Las otras opciones son incorrectas ya que no son las extensiones estándar utilizadas para este propósito en LDAP.

7. ¿Qué comando se utiliza para añadir entradas al directorio LDAP?

A. ldapinsert

\_ B. ldapadd

C. ldapupdate

D. ldapput

La opción B es correcta. El comando "ldapadd" se utiliza para añadir nuevas entradas al directorio LDAP, Ldapmodify se usa para modificar entradas existentes en el directorio LDAP, ldapsearch permite buscar y recuperar entradas del directorio LDAP,

ldapdelete se usa para eliminar entradas del directorio LDAP.

8. ¿Qué significa OU en la estructura de LDAP?

A. Original User

\_ B. Organizational Unit

C. Output Unit

D. Operational Utility

La opción B es correcta. OU significa Organizational Unit (Unidad Organizativa) en la estructura de LDAP. Las otras opciones son incorrectas ya que no representan el significado correcto de OU en el contexto de LDAP.

9. ¿Qué comando se utiliza para generar una contraseña encriptada para un usuario LDAP?

A. ldappasswd

B. encryptpass

\_ C. slappasswd

D. hashpassword

La opción C es correcta. El comando "slappasswd" se utiliza para generar una contraseña encriptada para un usuario LDAP. En el caso de las respuestas B y D no son comandos reales de LDAP, la respuesta A es un comando real, pero para cambiar la contraseña de una entrada sin cifrarla.

10. ¿Qué atributo se utiliza para especificar el nombre común de un usuario en LDAP?

A. username

B. fullname

\_ C. cn

D. name

La opción C es correcta. El atributo "cn" (Common Name) se utiliza para especificar el nombre común de un usuario en LDAP. Las opciones A y B son incorrectas ya que no son los atributos estándar de LDAP. En el caso de name aunque es descriptivo, no es el atributo LDAP específico para el nombre común.

11. ¿Qué significa DIT en el contexto de LDAP?

A. Data Information Type

B. Directory Integration Tool

\_ C. Directory Information Tree

D. Data Interchange Technology

La opción C es correcta. DIT significa Directory Information Tree (Árbol de Información de Directorio) en el contexto de LDAP. Las otras opciones son incorrectas ya que no representan el significado correcto de DIT en LDAP.

12. ¿Qué comando se utiliza para buscar y recuperar entradas del directorio LDAP?

A. ldapfind

B. ldapquery

\_ C. ldapsearch

D. ldapget

La opción C es correcta. El comando "ldapsearch" se utiliza para buscar y recuperar entradas del directorio LDAP. El resto de los comandos no son estándar en LDAP.

13. ¿Qué atributo se utiliza para especificar la contraseña de un usuario en un archivo LDIF?

A. password

B. pass

\_ C. userPassword

D. ldapPassword

La opción C es correcta. El atributo "userPassword" se utiliza para especificar la contraseña de un usuario en un archivo LDIF. Las otras opciones son incorrectas ya que no son los atributos estándar utilizados para este propósito en LDAP.

14. ¿Qué comando se utiliza para modificar entradas existentes en el directorio LDAP?

A. ldapchange

B. ldapupdate

\_ C. ldapmodify

D. ldapedit

La opción C es correcta. El comando "ldapmodify" se utiliza para modificar entradas existentes en el directorio LDAP. Las otras opciones no son los comandos estándar en las operaciones LDAP (ldapchange, ldapupdate, ldapedit).

15. ¿Qué significa DC en la estructura de nombres distinguidos de LDAP?

A. Directory Component

\_ B. Domain Component

C. Data Category

D. Directory Category

La opción B es correcta. DC significa Domain Component (Componente de Dominio) en la estructura de nombres distinguidos de LDAP. Las otras opciones no representan el significado correcto de DC en el contexto de LDAP.

16. ¿Qué comando se utiliza para eliminar entradas existentes en el directorio LDAP?

A. ldapremove

B. ldaperase

\_ C. ldapdelete

D. ldapcut

La opción C es correcta. El comando "ldapdelete" se utiliza para eliminar entradas existentes en el directorio LDAP. Las otras opciones no son los comandos existentes en LDAP.

17. ¿Qué atributo se utiliza para especificar el identificador único de un usuario en LDAP?

A. id

B. uid

C. cn

\_D. uid o uidNumber

La opción D es la más correcta y completa. El atributo "uid" (User ID) es un identificador único textual, a menudo el nombre de usuario, "uidNumber” es un identificador numérico único, similar al UID en sistemas Unix. La opción B (uid) es parcialmente correcta, pero no incluye uidNumber. La opción A (id) no es un atributo estándar en LDAP. La opción C (cn, Common Name) se usa para el nombre del usuario, no como identificador único.

18. ¿Qué protocolo utiliza LDAP para la comunicación en red?

A. HTTP

B. FTP

\_ C. TCP/IP

D. SMTP

La opción C es correcta. LDAP utiliza TCP/IP para la comunicación en red. Las otras opciones son incorrectas: HTTP es un protocolo de aplicación para la web, FTP es para transferencia de archivos, y SMTP es para correo electrónico. Ninguno de estos es el protocolo de transporte utilizado por LDAP.

19. ¿Qué significa SSHA en el contexto de contraseñas LDAP?

A. Secure Shell Authentication

B. Simple Secure Hashing Algorithm

\_ C. Salted Secure Hash Algorithm

D. Symmetric Secure Hashing Authentication

La opción C es correcta. SSHA significa Salted Secure Hash Algorithm en el contexto de contraseñas LDAP. Las otras opciones no representan el significado correcto de SSHA en LDAP.

20. ¿Qué atributo se utiliza para especificar el directorio home de un usuario en LDAP?

A. homedir

B. userdir

\_ C. homeDirectory

D. ldapHome

La opción C es correcta. El atributo "homeDirectory" se utiliza para especificar el directorio home de un usuario en LDAP. Las otras opciones no son atributos estándar existentes en LDAP.

21. ¿Qué significa objectClass en un archivo LDIF?

A. Es el nombre de la clase Java asociada al objeto

B. Es una clasificación visual de los objetos en el directorio

\_ C. Define las características y propiedades del objeto en el directorio LDAP

D. Es el nombre de la tabla SQL donde se almacena el objeto

La opción C es correcta. objectClass define las características y propiedades del objeto en el directorio LDAP. Las otras opciones son incorrectas por las siguientes razones: LDAP no está relacionado con Java, no es una clasificación visual y LDAP no utiliza tablas SQL.

22. ¿Qué comando se utiliza para verificar la configuración del servidor LDAP?

A. ldapverify

B. checkldap

\_ C. slapcat

D. ldaptest

La opción C es correcta. El comando de verificación del servidor de directorios, conocido como "slapcat", se emplea para confirmar la configuración del mismo. Este comando muestra los detalles del directorio, abarcando entidades como organizaciones, grupos y usuarios, permitiendo así asegurar el registro adecuado de dichos elementos. El resto de los comandos no existen en LDAP.