

documentacion de codigo: directorio activo (ldap)

En lenguaje de programación Python.



19 de abril de 2017

UNIDAD DE SOPORTE DE LA FACULTAD DE MATEMÁTICAS

José Omar León Peraza, Israel Fuentes Brito

Contenido

[Introducción 2](#_Toc487026573)

[Razones por las cuales usar LDAP 2](#_Toc487026574)

[Objetivo del código 3](#_Toc487026575)

[Código 3](#_Toc487026576)

[Referencias 4](#_Toc487026577)

[Anotaciones y recomendaciones 4](#_Toc487026578)

# Introducción

Las siglas de LDAP significan “protocolo ligero de acceso a directorios”, es un conjunto de protocolos de distribución libre usados para acceder a información guardada centralmente a través de la red. Está basado en el estándar X.500 para compartir directorios, pero es menos complejo e intensivo en el uso de recursos. Por esta razón, a veces se habla de LDAP como "X.500 Lite." El estándar X.500 es un directorio que contiene información de forma jerárquica y categorizada, que puede incluir nombres, directorios y números telefónicos.

LDAP es un sistema cliente/servidor. El servidor puede usar una variedad de bases de datos para guardar un directorio, cada uno optimizado para operaciones de lectura rápidas y en gran volumen. Cuando una aplicación cliente LDAP se conecta a un servidor LDAP puede, o bien consultar un directorio, o intentar modificarlo. En el evento de una consulta, el servidor, puede contestarla localmente o puede dirigir la consulta a un servidor LDAP que tenga la respuesta. Si la aplicación cliente está intentando modificar información en un directorio LDAP, el servidor verifica que el usuario tiene permiso para efectuar el cambio y después añade o actualiza la información.

Sin embargo, en la mayoría de los casos, LDAP se usa simplemente como un directorio telefónico virtual, permitiendo a los usuarios acceder fácilmente la información de contacto de otros usuarios. Pero LDAP va mucho más lejos que un directorio telefónico tradicional, ya que es capaz de propagar su consulta a otros servidores LDAP por todo el mundo, proporcionando un repositorio de información ad-hoc global. Sin embargo, en este momento LDAP se usa más para organizaciones individuales, como universidades, departamentos del gobierno y compañías privadas.

Las bibliotecas LDAP están disponibles para Python, pero la más popular es el módulo Python-LDAP, que utiliza la biblioteca OpenLDAP como base para proporcionar acceso a la red a un servidor LDAP.

# Razones por las cuales usar LDAP

La mayor ventaja de LDAP es que se puede consolidar información para toda una organización dentro de un repositorio central. Por ejemplo, en vez de administrar listas de usuarios para cada grupo dentro de una organización, puede usar LDAP como directorio central, accesible desde cualquier parte de la red. Puesto que LDAP soporta la Capa de conexión segura (SSL) y la Seguridad de la capa de transporte (TLS), los datos confidenciales se pueden proteger de los curiosos.

LDAP también soporta un número de bases de datos back-end en las que se guardan directorios. Esto permite que los administradores tengan la flexibilidad para desplegar la base de datos más indicada para el tipo de información que el servidor tiene que diseminar. También, ya que LDAP tiene una interfaz de programación de aplicaciones (API) bien definida, el número de aplicaciones acreditadas para LDAP son numerosas y están aumentando en cantidad y calidad.

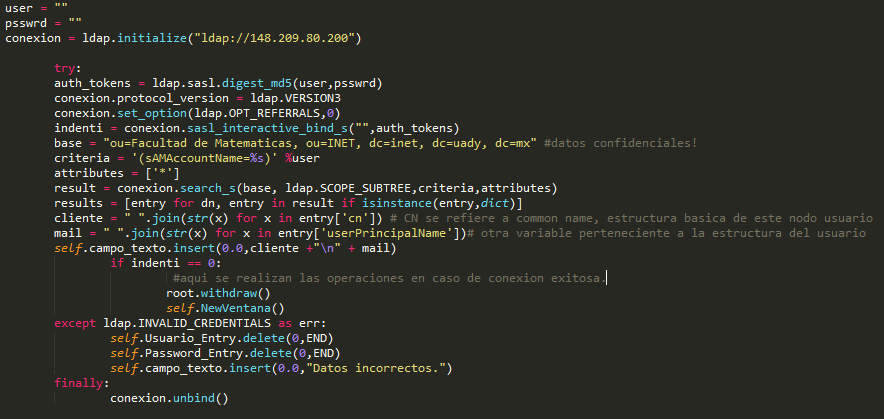
# Objetivo del código

Python-ldap proporciona una API orientada a objetos para acceder a los servidores de directorio LDAP de los programas Python, el objetivo del código es presentar una función para poder conectarse al directorio activo de la Facultad, cabe recalcar que los datos presentados en el código fuente son de carácter **CONFIDENCIAL.**

**NOTA**: Es recomendable para entender mejor el código, investigar sobre la herramienta OpenLdap, en ella se podrá conocer sobre la teoría de la creación de un directorio, estructuras básicas de un directorio o nodos, hasta ejemplos para el lector sobre como configurar un sistema operativo de Linux para acceder a este por medio de cuentas creadas de un directorio.

# Código

Ldap se utiliza para crear “logins”, para manipular entradas del directorio activo o realizar consultas, para esta función de acceso se requiere comenzar con una conexión al servidor donde se encuentra el directorio activo de la escuela, acto seguido en un bloque “try” se realiza la configuración de parámetros para mandar la solicitud de consulta al servidor. Se puede observar que se manejan excepciones en caso de que las matriculas estén erróneas y al final es importante cerrar la conexión al servidor.



Función Conectar\_Ldap 1

Para realizar la conexión se utiliza la versión 3 del protocolo de ldap, es un parámetro importante que requiere ser declarado, al igual que la base, la **base** de un directorio activo sirve como nombre de dominio general, es usado para identificar a las bases de datos y también sirve como dirección de búsqueda sobre los datos a los que apuntamos a consultar, esto se debe a que los directorios activos tienen estructura de árbol y se requiere una base que defina a que nodos (unidades organizacionales = OU y nombre de dominio = dc), es muy importante que esta variable este correcta ya que en caso contrario no se podrá localizar el directorio.



1. Base del directorio activo de FMAT

Continuando con la explicación del código se introduce una consulta a la base de datos como sigue:



Consulta en Ldap 1

Se declara como en la imagen, una variable asignada al resultado de la llamada a la función “search\_s” de un tipo de dato que previamente (en este caso la variable fue: conexión) haya realizado una conexión al directorio, se pasan como parámetros la base, ldap.scope\_subtree (dato predeterminado), la criteria y los atributos de la búsqueda, en este caso se utilizó como criterio de búsqueda a todos los datos de tipo usuario pertenecientes al directorio, y como atributos se uso ninguno.

El resultado se devuelve como texto plano, entonces es necesario descomponerlo en tokens que sean los objetos de nuestro interés, lo que se realiza en la segunda línea de la imagen Consulta en Ldap 1, es colocar el resultado en un a matriz “entry” para poder acceder a la información como las siguientes líneas hacen referencia.

Por ejemplo para poder obtener el nombre del usuario se hace una concatenación de un espacio “ ” con el resultado en la matriz que concuerde con la tupla de “CN” o common name, como este existen más variables que conforman la estructura de en este caso nuestro usuario como podría ser el correo electrónico que en este caso está vinculada a la tupla ‘userPrincipalName’.

# Referencias

* Red Hat Enterprise Linux 4: Manual de referencia
* https://www.openldap.org

# Anotaciones y recomendaciones

* Se recomienda estudiar la teoría sobre directorios activos y sus estructuras básicas