**LDAP**

**LDAP** significa Lightweight Directory Access Protocol

* protocolo leve para acessar serviços de diretório.
* roda em cima do protocolo TCP/IP.
* arquitetura cliente/servidor
* foi inicialmente usado como uma interface para o X.500
* Organiza as entradas em árvores hierárquicas;
* camada de aplicação

O **OpenLDAP** é um [*software*](https://pt.wikipedia.org/wiki/Software) [livre](https://pt.wikipedia.org/wiki/Software_livre) de [código aberto](https://pt.wikipedia.org/wiki/Open_source) que implementa o protocolo [LDAP](https://pt.wikipedia.org/wiki/LDAP). Ele é um [serviço de diretório](https://pt.wikipedia.org/wiki/Servi%C3%A7o_de_diret%C3%B3rio) baseado no padrão [X.500](https://pt.wikipedia.org/wiki/X.500).

O OpenLDAP é independente de [sistema operativo](https://pt.wikipedia.org/wiki/Sistema_operativo). Várias distribuições [Linux](https://pt.wikipedia.org/wiki/Linux) incluem o pacote do OpenLDAP. O software também corre nos sistemas operativos [BSD](https://pt.wikipedia.org/wiki/Berkeley_Software_Distribution), [AIX](https://pt.wikipedia.org/wiki/Advanced_Interactive_eXecutive), [HP-UX](https://pt.wikipedia.org/wiki/HP-UX), [Mac OS X](https://pt.wikipedia.org/wiki/Mac_OS_X), [Solaris](https://pt.wikipedia.org/wiki/Solaris), [Microsoft Windows](https://pt.wikipedia.org/wiki/Microsoft_Windows) (2000, XP, 2003, 2008, Vista, win7 e win 8) e [z/OS](https://pt.wikipedia.org/wiki/Z/OS).

O OpenLDAP foi desenvolvido inicialmente pela Universidade de Michigan com as seguintes características principais:

* suporte a [IPv4](https://pt.wikipedia.org/wiki/IPv4) e [IPv6](https://pt.wikipedia.org/wiki/IPv6);
* autenticação (**Cryrus Sasl-Kerberos V**, **GSSAPI**, **Digest-MD5**);
* segurança no transporte – [SSL](https://pt.wikipedia.org/wiki/SSL) e [TLS](https://pt.wikipedia.org/wiki/TLS);
* controle de acessos;
* escolha entre banco de dados;
* capacidade de atender a múltiplos bancos de dados simultaneamente;
* alta performance em múltiplas chamadas;
* replicação de base;

Um diretório LDAP geralmente segue o modelo X.500, que é uma árvore de nós, cada um consistindo de um conjunto de atributos com seus respectivos valores. O LDAP foi criado como uma **alternativa ao Directory Access Protocol**(DAP).

O diretório do LDAP nas distribuições debian e afins é **/etc/ldap** já nas distribuições baseadas em red-hat centos o diretorio é /etc/openldap.

Basicamente o arquivo de configuração do ldap pode ser feito no arquivo **slapd.conf** ou então pode se criar as configurações a partir de arquivos LDIFs e adicionar essas configurações ao DIT, essa configuração é conhecida como on the fly, ou seja depois de cada configuração do servidor LDAP não precisa reiniciar o serviço.

Essas configurações são feitas tanto em distribuições debian quanto red-hat.

Um cliente começa uma sessão de LDAP ligando-se a um servidor LDAP, normalmente pela porta padrão 389 TCP. Este envia requisições para o servidor, o qual devolve respostas. As operações básicas são:

**Bind – AUTENTICA e ESPECIFICA a versão do protocolo LDAP;**  
Unbind – fecha a conexão, não o inverso de Bind.  
Abandon – aborta uma requisição prévia;  
Search – procura por e/ou recupera entradas dos diretórios;  
Compare – testa se uma entrada tem determinado valor como atributo;  
Add – adiciona uma nova entrada;  
Delete – apaga uma entrada;  
Modify – modifica uma entrada;  
Modify DN – move ou renomeia uma entrada;  
StartTLS – protege a conexão com a Transport Layer Security (TLS);  
Extended Operation – operação genérica para definir outras operações;

O LDAP usa SSL e TLS:

**LDAP Over SSL vs LDAP with STARTTLS**

There are two ways to encrypt LDAP connections with SSL/TLS.

Traditionally, LDAP connections that needed to be encrypted were handled on a separate port, typically 636. The entire connection would be wrapped with SSL/TLS. This process, called LDAP over SSL, uses the ldaps:// protocol. This method of encryption is now deprecated.

STARTTLS is an alternative approach that is now the preferred method of encrypting an LDAP connection. STARTTLS "upgrades" a non-encrypted connection by wrapping it with SSL/TLS after/during the connection process. This allows unencrypted and encrypted connections to be handled by the same port. This guide will utilize STARTTLS to encrypt connections.

**Active Directory**

Para que os usuários possam acessar os recursos disponíveis na rede, estes deverão efetuar o logon. Quando o usuário efetua logon, o AD verifica se as informações fornecidas pelos usuários são válidas, e em caso positivo, faz a autenticação. O AD é organizado de uma forma hierárquica, com o uso de domínios. Caso uma rede utilize o AD, poderá conter vários domínios. Um domínio é nada mais do que um limite administrativo e de segurança, ou seja, o administrador do domínio possui permissões somente no domínio, e não em outros domínios. As políticas de segurança também se aplicam somente ao domínio, e não a outros domínios. Resumindo: diferentes domínios podem ter diferentes administradores e diferentes políticas de segurança.

Nos domínios baseados no AD, podemos ter dois tipos de servidores: Controlador de Domínio (DC – Domain Controller) e Servidor Membro (Member Server).

O LDAP nativo roda na porta 389/TCP e não implementa recursos de segurança. Entretanto, pode-se utilizar recursos de segurança de maneira estendida, como pela criação de túneis TLS para tal finalidade. Nesse caso, muda-se inclusive, a porta de operação do protocolo, também conhecido como LDAPS – 636/TCP. Pode-se verificar tais informações diretamente nas RFCs do LDAP: 4511 – Definição do protocolo e 4513 – Mecanismos de autenticação.

**OAuth**é um padrão aberto para autorização, comumente utilizado para permitir que os usuários da Internet possam fazer logon em sites de terceiros usando suas contas do Google, Facebook, Microsoft, Twitter, etc.—mas, sem expor sua senha.[1] Geralmente, o OAuth fornece aos clientes um "acesso seguro delegado" aos recursos do servidor em nome do proprietário do recurso. Ele especifica um processo para proprietários de recursos para autorizar o acesso de terceiros aos seus recursos de servidor sem compartilhar suas credenciais. Projetado especificamente para trabalhar com o Protocolo de Transferência de Hipertexto (HTTP), o OAuth permite essencialmente tokens de acesso a ser emitidos para clientes de terceiros, mediante autorização do servidor, com a aprovação do proprietário do recurso. O terceiro, em seguida, usa o token de acesso para recursos protegidos hospedados pelo servidor.