### LDAP协议

LDAP（Light Directory Accesss Protocol）是基于x.500的轻量级目录访问协议，目录服务是一个特殊的数据库，用来保存描述性的、基于属性的信息（比如用户账号信息，也可把LDAP当成用户信息数据库），目录数据库的读性能优异，写性能较差。

常见的目录数据库有微软的Active Directory活动目录，OpenLdap开源的

LDAP记录中的关键字：

|  |  |
| --- | --- |
| DC | Domain Component域名的部分，将完整的域名以.分割成几部分  如cof.com的DC记为： dc=cof,dc=com |
| OU | Organization Unit组织单位，表示一个用户组 |
| CN | Common Name通用名称，常表示最终用户名称 |
| DN | Distinguished Name 每一个记录条目唯一的标识名，完整的  如： cn=userxx,ou=comp1,dc=cof,dc=com |
| RDN | Relative DN相对辨别名，DN最左边的，如 cn=userxx |
| BaseDN | DN右边的dc部分，如 dc=cof,dc=com |
| UPN | User Principal Name，如 userxx@cof.com |

查询操作：搜索，比较

更新操作：添加条目，删除条目，修改条目值，修改条目名

认证操作：绑定，解绑定

其他：放弃，扩展操作