Configuring and installing LDAP:

LDAP stands for Lightweight Directory Access Protocol.

LDAP is a solution to access centrally stored information over network. This centrally stored information is organized in a directory that follows X.500 standard.

The information is stored and organized in a hierarchical manner and the advantage of this approach is that the information can be grouped into containers and clients can access these containers whenever needed.

The OpenLDAP hierarchy is almost similar to the DNS hierarchy.  
  
The following are the two most commonly used objects in OpenLDAP:

1. cn (common name) – This refers to the leaf entries, which are end objects (for example: users and groups)
2. dc (domain component) – This refers to one of the container entries in the LDAP hierarchy. If in a setup the LDAP hierarchy is mapped to a DNS hierarchy, typically all DNS domains are referred to as DC objects.

For example, if there is user in the hierarchy sam.thegeekstuff.com, the fully distinguished name of this user is referred as cn=sam, dc=thegeekstuff, dc=com. If you noticed in the FDN (fully distinguished name), a comma is used a separator and not a dot, which is common in DNS.

By using the different LDAP entry types, you can setup a hierarchical directory structure. This is the reason why openLDAP is so widely used. You can easily build an openLDAP hierarchy where objects in the other locations are easily referred to without storing them on local servers. This makes OpenLDAP a lightweight directory, especially when compared to other directory servers such as Microsoft’s Active directory.

Now lets see how to setup a single instance of an LDAP server that can be used by multiple clients in your network for authentication