How to create an LDAP server instance

How-to Guide
How to create an LDAP server instance

1. Login to the Pulse Secure Application Gateway/Controller
2. Go to Authentication>Auth. Servers
3. From the new server drop down, select LDAP; click on New
4. Provide the name of the server; this should have meaning to the administration team
5. Provide the primary LDAP server IP address (if desired and resolution can be confirmed 100% of the time, hostname can be used); define the backup server details if desired
6. Define the port that should be used; default LDAP is 389; custom ports can be used if desired (for example, 3689 for the Global Catalog port)
7. Choose the LDAP server type (for the purposes of this guide, AD will be used; minor changes are needed for the other server types; the LDAP admin should provide the correct values)
   a. Generic: Not one of the server types that is pre-defined
   b. Active Directory: used to communicate to a Windows server running Active Directory Services
   c. iPlanet: Used to connect to a Sun iPlanet server
   d. Novell eDirectory: used to connect to a Novell server
8. Connection Timeout: the time (in seconds) that the device should attempt to connect to the LDAP server(s) prior to recording as unreachable and fallback to the next server (if configured)
9. Search timeout: Length of time to wait for the server to return the answer to the query
10. Authentication required:
    a. If the LDAP server requires authentication for queries/access, enable the option to authenticate to search (this should be enabled unless directed otherwise by the LDAP administrator)
    b. Admin DN: the LDAP name of the admin (e.g. cn=admin,cn=users,dc=domain,dc=com)
    c. Admin password: the password of the user
11. Finding user entries:
    a. Base DN: Fill out the location users reside in the directory structure
    b. Filter: how the user is defined (e.g. CN=<sAMAccountName>; O=<user>; C=<username>)
12. Determine Group membership:
    a. Base DN: location where groups are stored on the directory structure. This can be at the root or further down the tree; search does not traverse up)
    b. Filter: how the group is defined (e.g cn=<GROUPNAME>
c. Member attribute: directory server value for the user being a member of the group. This applies to static groups.
   i. Reverse group search: When enabled, the information on the group is checked from the user attribute prior to searching for all groups and if the user is a member of the group

d. Query attribute: the values in the directory server for dynamic groups

e. Nested group level: The number of groups that can be in groups

f. Nested group search (the higher the values, the more impact to the system)
   i. Nested groups in catalog will limit the query to only the number of groups of the group level value
   ii. Search all nested groups: nesting will be done through the end of the path. (Please note, there is a performance decrease as the number of nested groups increases.)