Task 3 - Get basic LDAP information

Part A: Discussion Items

Ask the *LDAP administrator* for the following information. *Items 1-6 are required*. The remainder are optional, in that you may deduce them during the subsequent tasks or use the defaults in most environments. As a best practice, verify any items deduced by simple clients with your LDAP administrator prior to relying on them in your application, particularly in production environments.

1. **Required:** LDAP type and version. For example, *IBM Tivoli Directory Server v6.1*.

   ____

2. **Required:** Fully qualified host name of the LDAP server. For example, *ldapserver.hcl.com*.

   ____

3. **Required:** LDAP port - *389* is the default non-SSL port and *636* is the default SSL port (TLS port) for LDAP, from the Internet Assigned Numbers Authority. If non-SSL, how is the network secured?

   ____

4. **Required:** If HCL Portal must communicate with the LDAP over SSL, the LDAP administrator may provide an SSL certificate to enable this. Optionally, WebSphere Application Server can pull the certificate from the LDAP server itself.

   ____

5. **Required:** Base distinguished name or names (DN) – This is the entry point for VMM into the LDAP. Any data that HCL Portal needs should reside under this node in the directory information tree (DIT) of the LDAP. Note that base DNs should not overlap in VMM realms. For example, *o=hcl,c=us*.

   ____

6. **Required:** LDAP bind user and password – The LDAP administrator should provide the full DN of the bind user. The bind user is the identity that HCL Portal via underlying VMM uses to connect to the LDAP. For example, *cn=root*.

   ____

   ____

7. Will HCL Portal access the LDAP server directly or through any load balancer, firewall, or proxy? If not directly, does the load balancer, firewall, or proxy impose any idle timeout or otherwise limit TCP connections made through it? Does the LDAP itself restrict the total number of TCP connections per application? Should the total number of TCP connections per application be restricted for LDAP performance reasons?

    ____

    ____

    ____

8. If not through a load balancer, should VMM fail over to some backup LDAP server when the primary server is not available? If so, confirm that the backup is an exact replica, including universally unique identifier (UUID) values (RFC 3928).

    ____

    ____

9. A detailed explanation of the access rights that the bind user has on nodes, users, and groups under the base DN. Note that VMM acts as the bind user during every interaction with the LDAP except for verifying a specific user's password during the login process. Specifically, you must establish whether the bind user can:

    - Create and delete users

    ____

    - Update existing users

    ____

    - Create and delete groups

    ____

    - Update existing groups

    ____

10. What object class(es) defines users in this LDAP? Does the LDAP store all users under a specific node in its DIT?

    ____

____

- Provide an LDIF of a sample user. See Task 7, #3.

11. What object class(es) defines groups in this LDAP? Does the LDAP store all groups under a specific node in its DIT?

____

____

- Provide an LDIF of a sample group. See Task 7, #3.
- If the LDAP includes both static and dynamic groups, provide an LDIF of each.
- Does the LDAP allow you to create empty groups? Or must any new group include at least one member?

____

12. Does the LDAP implement a group membership attribute? If so, what is it and what is its scope? By *scope*, does it resolve direct groups only; direct and nested groups; or dynamic, direct, and nested groups? For example, in IBM Tivoli Directory Server, *ibm-allGroups*.

____

____

13. Does the LDAP implement dynamic groups? If so, what object class defines these? And what is the dynamic member attribute (which attribute stores the URL that defines the group)?

____

____

- Note that dynamic groups generally impose a high performance overhead on both HCL Portal and the LDAP, so the LDAP will ideally resolve these to group membership attribute values.

14. What is the UUID and can it be searched externally? Reference Article KB0012799.

____

15. Does the LDAP rely on LDAP referrals to serve any requests?

____