**Lab01-Document**

**Setting up Management Authentication and Authorization for IBM Access Manager**

Setting lab environment: We need to select virtual machine to perform the tasks in the lab. There are user VM, IBM Access Manager Appliance VM, IBM Directory Server Appliance VM.

**LDAP Structure Overview:**

* IBM Directory Server Appliance VM includes an organized LDAP instance. The LDAP instance includes users and groups set up.
* LDAP instance has two groups: admins and auditors
* The admins group includes two user members: admin and binduser
* The auditors group has two user members: bob and peter

**Starting LDAP:**

* Select ‘iamd’ virtual machine and login with username as ‘admin’ and password as ‘P@ssw0rd’
* Open this url in a firefox browser ‘https://sds1.com’ and login with ‘admin’ and ‘P@ssw0rd’
* Under ‘Server Control’ section, select ‘Directory Server’ and click on ‘Start’ button

**Configuring Management Authentication:**

* **Setting up management authentication**: Navigate to ‘https://iamidpa.ibmemm.edu’ and login with ‘admin’ and ‘P@ssw0rd’
* Navigate to ‘Manage System Settings >System Settings>Management Authentication’
* Select ‘Remote LDAP User Registry’ and in next LDAP tab enter host name as ‘sds1.com’ and port number as ‘389’
* Uncheck ‘Anonymous Bind’, in Bind DN field enter ‘cn=binduser,ou=adminusers,o=myorg,c=us’ and Bind Password as ‘P@ssw0rd’
* In LDAP General tab, ‘Group Member Attribute field’, enter ‘uniquemember’ and ‘Base DN field’, enter ‘c=us’.
* Leave default settings in LDAP SSL tab and save
* To deploy the changes, click on ‘Click here to review the changes or apply them to the system’ then select ‘Deploy’ option and logout
* **Login as an external user** with credentials ‘admin’ and ‘object00’ and as **local user** with credentials ‘admin@local’ and ‘P@ssw0rd’

**Configuring Management Authorization:**

* **Setting up management authorization**: Navigate to ‘https://iamidpa.ibmemm.edu’ and login with ‘admin@local’ and ‘P@ssw0rd’
* Navigate to ‘Manage System Settings >System Settings>Management Authorization’
* Check ‘Enable Authorization Roles’ and click on Click here to review the changes or apply them to the system’ then select ‘Deploy’ option and logout
* Navigate to ‘Manage System Settings >System Settings>Management Authentication’ and click on LDAP tab and Bind Password field, type P@ssw0rd
* In LDAP General tab, Administrative Group DN field, update to ‘ou=groups,o=myorg,c=us’
* In LDAP SSL tab, leave the default settings then save and deploy
* Navigate to Manage System Settings > System Settings: Management Authorization. In the Roles list, select Global Administrators
* In the right pane, click the ‘Remote LDAP User Registry’ Tab. Above the Group name area, click ‘Edit’. Click on Groups tab for the group name enter admins and search. Select admins is listed in the group name list
* Similar way, we have to add ‘auditors’ and verify in the groups list.
* **Testing the auditors authorization**: Navigate to Secure Web Settings > Manage: Runtime Component and click on ‘Restart’
* **Testing the admin authorization**: Navigate to Secure Web Settings > Manage: Runtime Component and click on ‘Restart’