### Management Authentication and Authorization for IBM Access Manager

In File transfer or IBM SAM, External Authentication frequently refers to the use of LDAP or other Directory services. External Authentication server provides username and password information required for authentication.

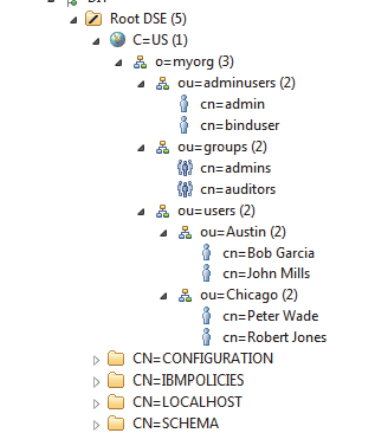
Here We are trying to implement or configure management authentication and authorization using IBM Secure Directory Suite Appliance as an external Active Directory.

We are hosting Security Access Manager Appliance on the IP address 192.168.42.196 and host name as iamidpa.ibmemm.edu. This Appliance VM has all the components required to keep the ISAM appliance up and running. Servers like Embedded LDAP server internal to the appliance, Reverse Proxy Server to host the junctions required for protection of objects. This server acts as Identity Provider.

The external Active Directory Server i.e. the LDAP server in this set up is IBM Secure Directory Suite Appliance and it is hosted over the IP address 192.168.42.111, with host name as sds1.com.

One user virtual machine is used to configure and test all these components. It has a browser and terminal in it to perform required operations.

IBM Directory server appliance VM includes an LDAP instance organized and the LDAP DIT is as follows:



ROOT DSE = Contains all information about the capabilities of the server and the data that it contains, and all information about the Directory Information Tree of LDAP files also known as ldif files.

In an LDAP directory record, C= country

dn= distinguished Name

dc = domain component

ou= organizational unit, group

o = organization

cn= common name

CN= Container Name

**AIM: Our main aim of this lab is to use SDS as LDAP server used for external authentication. And configure ISAM in a way to let the groups and users in this external LDAP server be allowed to access the protected resources based on their level of authentication. You use data or entries from the external LDAP for authn and authz over ISAM appliance.**

## Step 1: Starting LDAP

For configuration purposes, in the entire duration of the lab, we use just the user VM.

Firstly, login to the VM using username and password, then open the browser and open the link

htps://sds1.com, this is used to login to the LMI of IBM SDS. There in the **Server Control** module 🡪 Select **Directory Server** and Click on **Start.** Then you will be prompted to deploy the changes. In this way you are making the SDS LDAP server ready to access or to be used as active directory for external authentication.

## Step 2: Configuring management authentication

In this we configure management authentication over the ISAM appliance with external LDAP server, and then verify if users can access the LMI for ISAM.

### Setting up management authentication:

Logon to LMI of ISAM as admin.

In the LMI go to Manage System Settings module in that System Settings in that Management Authn

**Manage System Settings🡪 System Settings: Management Authn.**

Select the **Remote LDAP user registry** as option

Then give the required metadata to configure LDAP properly.

Metadata like Host Name (Here we are using SDS as LDAP server so Hostname is sds1.com), Port(389), Deselect Anonymous Bind upon performing that you will be prompted to add the **Bind Distinguished Name (DN)**, and Specify the **Bind Password.**

Configure **LDAP General** (with required metadata such as **user attribute**, **Group member Attribute**, **Administrative group DN**) and in LDAP SSL (in this lab we leave it to default) fields and Save and Close.

Then Deploy the changes. **Then *logout* as *admin* user**.

**Testing:** Login as an external user, as one mentioned on can be authenticated with external LDAP server. The external user we are using here which is present in external LDAP server is *admin* and password is *object00.* This step must be successful.

Login as local user the one present in embedded LDAP which is *admin@local* and *default* Password. These steps are success which means that *external* *authentication* is setup efficiently.

## Step 3: Configuring Management Authorization

We use the local user credentials to log into the LMI of ISAM, i.e. *admin@local.* Go to Management Authorization selection present in Manage System settings module. Click on Management Authorization🡪 enable authorization roles checkbox and deploy changes.

After this step again go to the Management Authentication tab in that select the Remote LDAP🡪 then let all the metadata previously provided be the same, except for in the **LDAP General 🡪**  change the **Administrative Group DN.** Save and Deploy the changes.

Go to the management Authorization selection in the ***Roles 🡪*** Select ***Global administrator***

Click the Remote LDAP user registry tab in the right pane and then in the **Group Name** field click edit and then **SEARCH** for admins. Add the group and Deploy the changes

Now got to ***Roles 🡪*** select ***Security Viewer.***

Click the Remote LDAP user registry tab in the right pane and then in the **Group Name** field click edit and then **SEARCH** for auditors. Add the group and Deploy the changes.

Logout of the ***admin@local*** user over the LMI.

## Step 4: Testing

Try logging in into the LMI using one user from the admins group and one user from the auditors group.

There must be difference in the LMI options accessible for both different users.

**Testing user from the** *auditors***group:** In this case we have one user in the auditors group as ***bob.*** On logging in as **bob** we can just see limited options over the LMI, we are unable to deploy few critical changes i.e. limited resource access. Hence correct level of access based on the authorization.

**Testing user from the** *admins***group:** In this case we have one user in the admins group as **admin.** On logging as **admin,** we try to do the actions forbidden by the auditors and all those can be successfully done.

Hence, we have successfully implemented Management Authentication and Management Authorization over IBM ISAM using external Active Directory such as IBM SDS with LDAP instance on it.