An Example for how to configure Role Based Management on

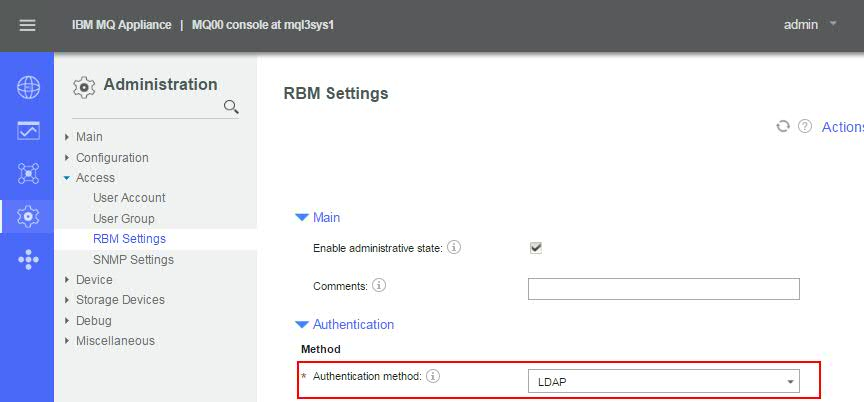
MQ Appliance to allow access to LDAP users

[Maya\_Anilson](javascript:;" \o "Maya_Anilson) |Apr 21 2017 Updated

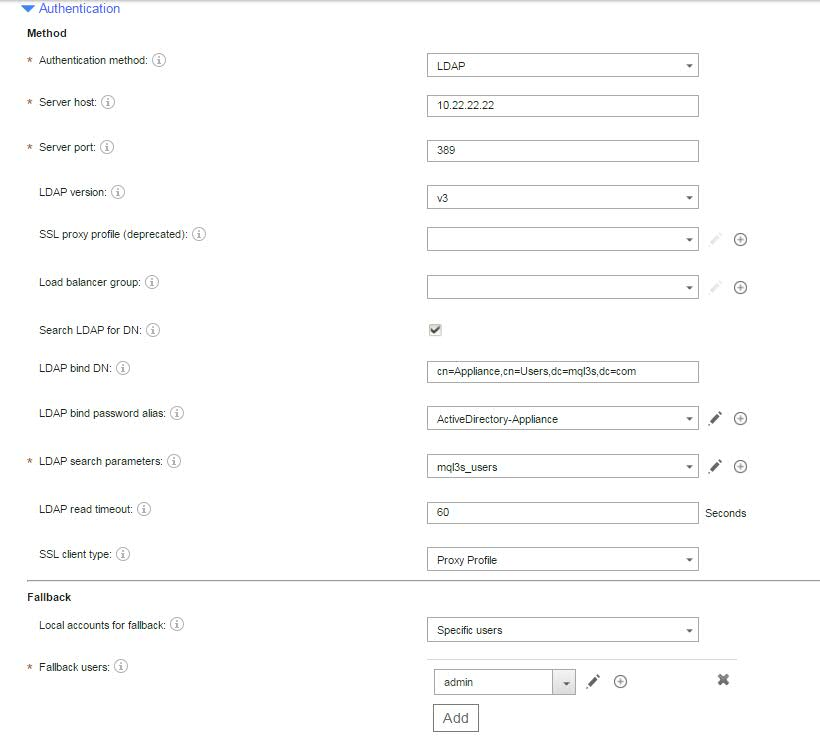
**An Example that shows how to configure Role Based Management (RBM) on MQ Appliance to allow access to LDAP users hosted on a Windows Active Directory.**

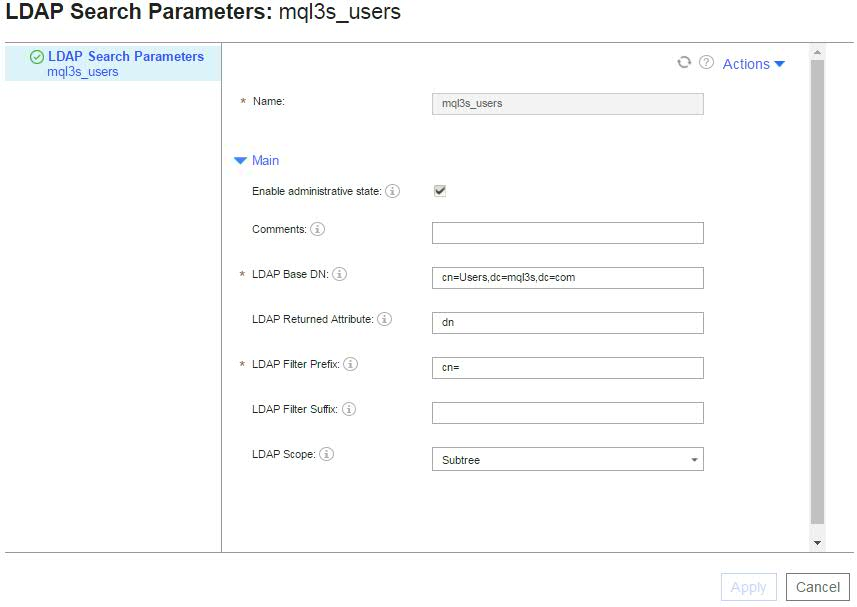
This article covers a pictorial walkthrough of configuring RBM with LDAP users accounts using WebUI to manage IBM MQ Appliance resources.

As a first step, I recommend reading Jamie’s blog which covers in detail various aspects of “Configuring LDAP Role-Based Management (RBM) on the IBM MQ Appliance” (see the related links at the end of this article).

* Log in to IBM MQ Appliance through WebUI using an admin id.
* Go to Settings  -> Access -> RBM Settings
* Under Authentication method choose LDAP
* Supply the host name or the IP address of the LDAP server.  The standard port for LDAP is 389 and the standard port for LDAPS is 636. Select appropriate LDAP version.
  + If you want the LDAP search to return the DN then check the option ‘Search LDAP for DN’.
  + If you want to use authenticated bind then specify a bind user account in the ‘LDAP bind DN’ and its password in the  ‘LDAP bind password alias’.  The LDAP search parameters should be provided with the information that we would like the LDAP search query to return.
* **Name:**  Provide a name for your LDAP search
* **LDAP Base DN:**    Set the base DN to search for users within the LDAP server
* **LDAP Returned Attribute:**  Specify the attribute that should be returned by your LDAP search query
* **LDAP Filter Prefix:**  Specify the LDAP prefix that the appliance prefixes the user name with when it is constructing a DN to pass to the LDAP server. The prefix is cn= by default.
* **LDAP Filter Suffix:**  Specify the LDAP suffix that the appliance appends to the user name when it is constructing a DN to pass to the LDAP server.

Sample authentication parameters look like this:





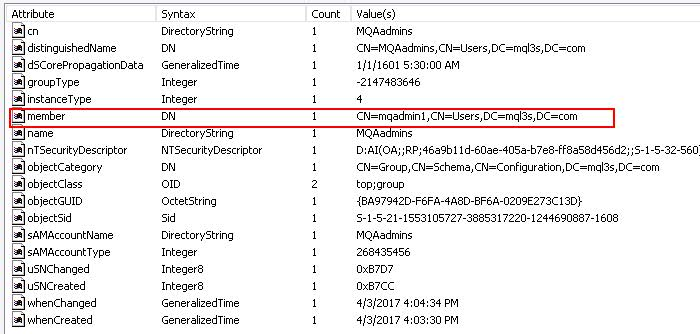
It is important to configure a local user account as a fallback user so that you can log in to the appliance with this account if the LDAP server becomes unavailable.

These settings ensures that when a user logs in to the appliance by providing a user account it is validated against the LDAP server to see if the userid and the password supplied matches the LDAP account and its password. The next step is to map the authenticated LDAP user to an access profile to determine what permissions this user account has on the MQ Appliance.

In this example I have created 2 LDAP groups MQAadmins and MQAguests. The users belonging to the MQAadmin account will have full access to all the MQ Appliance resources. The users belonging to the MQAguests will only have read access to the MQ Appliance resources.  So now I define my credential mapping in such a way that if the user account belonging to the MQAadmins group logs in then it is able to perform all administrative actions.

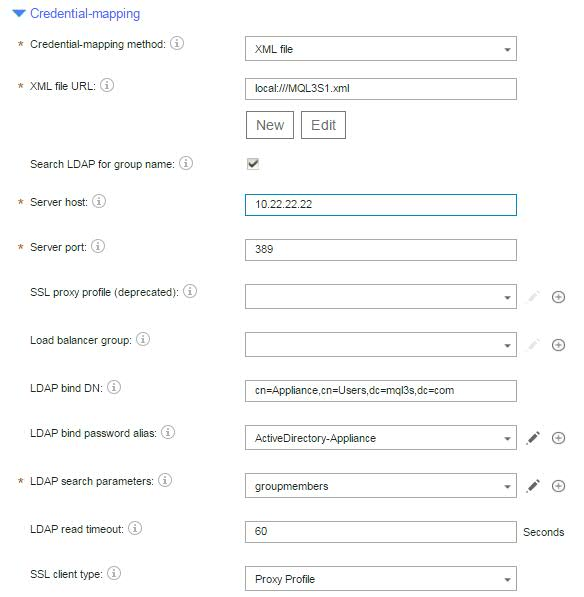
I am using XML file for mapping credentials and my XML file looks like the following:

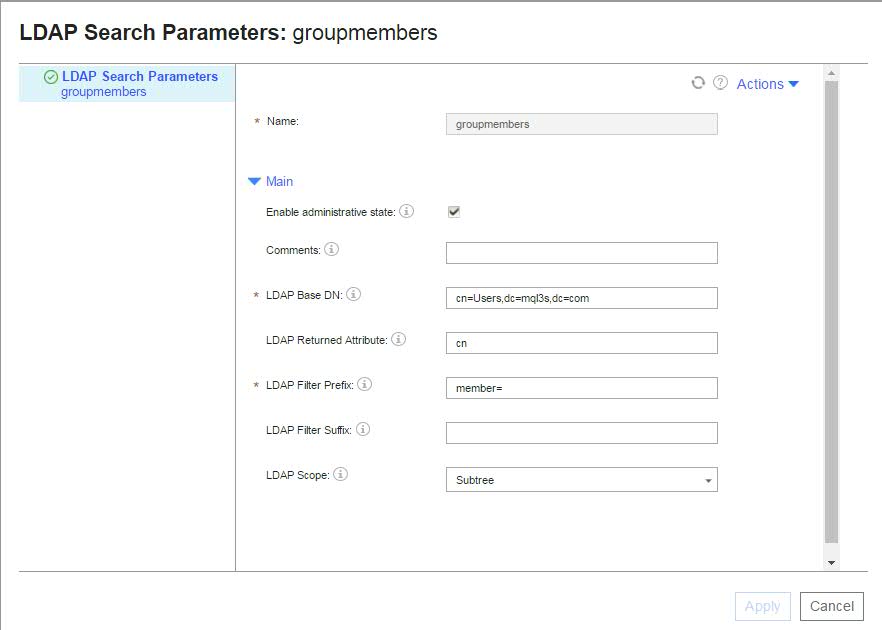
On my LDAP server the definition for MQAadmin group looks like this:



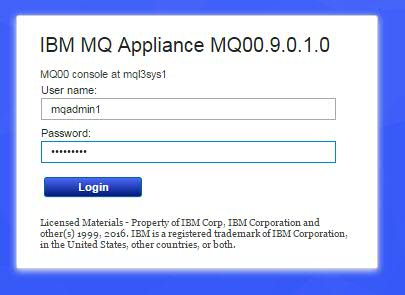
 Since I have set access policies for the LDAP groups I would want to enable the ‘Search LDAP for group names’.

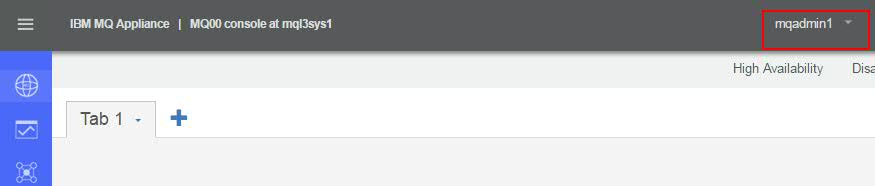
The LDAP search parameters that I use here is not the same that I used for authentication. This is because my LDAP search query for credential mapping is formulated in such a way that the LDAP server returns the groups to which the user account is a member.  Hence, I have set my LDAP prefix to ‘member=’ . The group names thus returned are compared with the credentials that I have set in my XML file.





Save the configuration and try to login to IBM MQ Appliance using  the LDAP user account.

[](https://www.ibm.com/developerworks/community/blogs/messaging/resource/BLOGS_UPLOADED_IMAGES/ldap_rbm_image8.png)

[](https://www.ibm.com/developerworks/community/blogs/messaging/resource/BLOGS_UPLOADED_IMAGES/ldap_rbm_image9.png)

With the above configuration I can now login to my MQ Appliance box with a user account mqadmin1 that belongs to MQAadmins group on the LDAP server.

**Related articles**

[Configuring LDAP Role-Based Management (RBM) on the IBM MQ Appliance](https://community.ibm.com/community/user/imwuc/viewdocument/configuring-ldap-role-based-managem?CommunityKey=183ec850-4947-49c8-9a2e-8e7c7fc46c64&tab=librarydocuments)

[User authentication with LDAP](https://www.ibm.com/support/knowledgecenter/en/SS5K6E_9.0.0/com.ibm.mqa.doc/security/se00070_.htm)