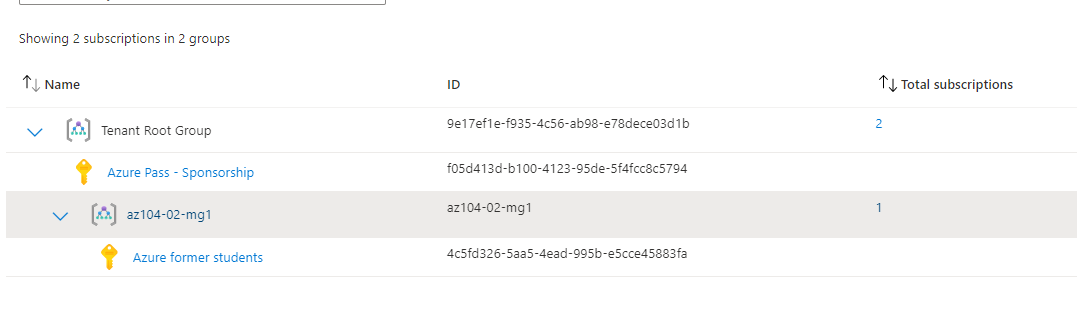
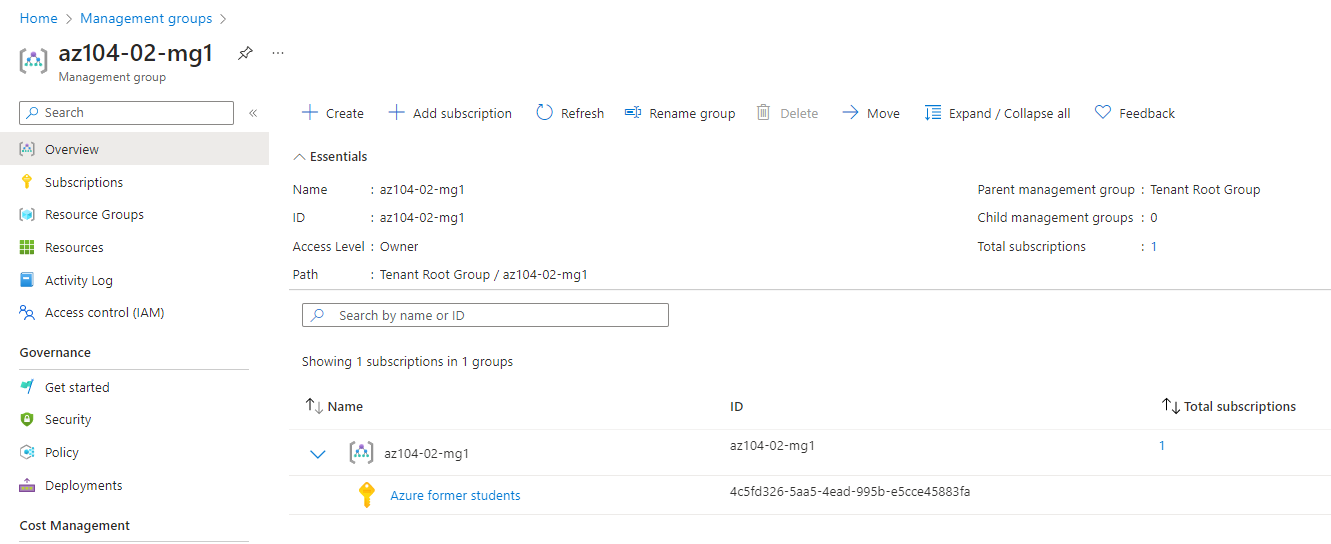
Lab Subcsriptions and RBAC – Lab 02a Manage Subcriptions and RBAC

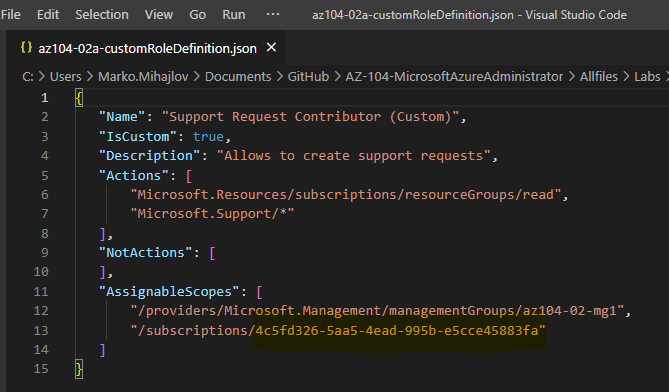
Task 1: Implement Management Groups

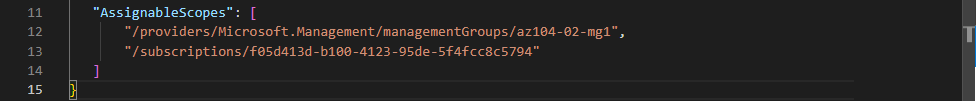


Creating the management group az-104-02-mg1 and adding my current subscription to the management group. Note that there is a root group named Tenant Root Group under which all other management groups fall under. As noted in the picture below Parent management group: Tenant Root Group



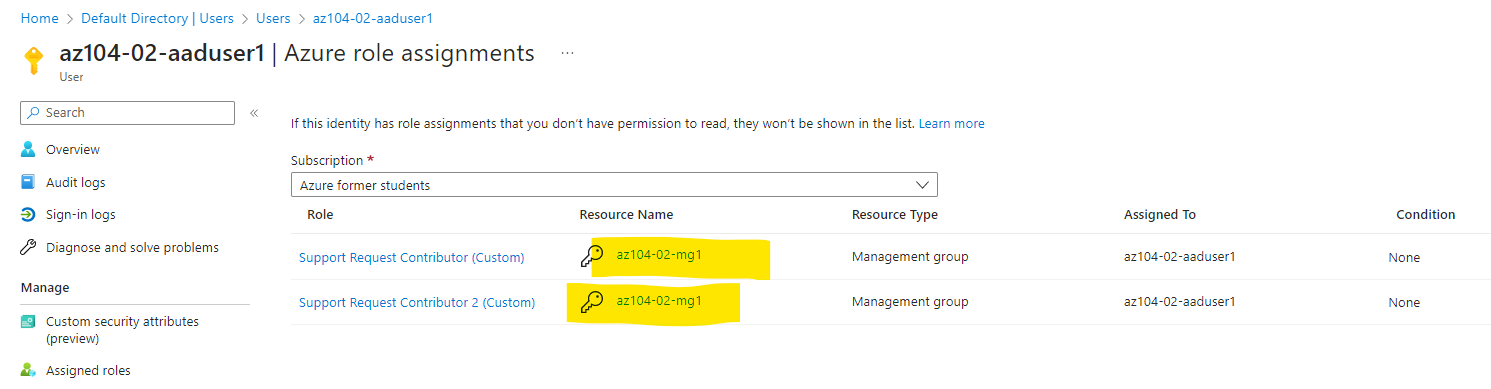
Task 2: Create custom RBAC roles





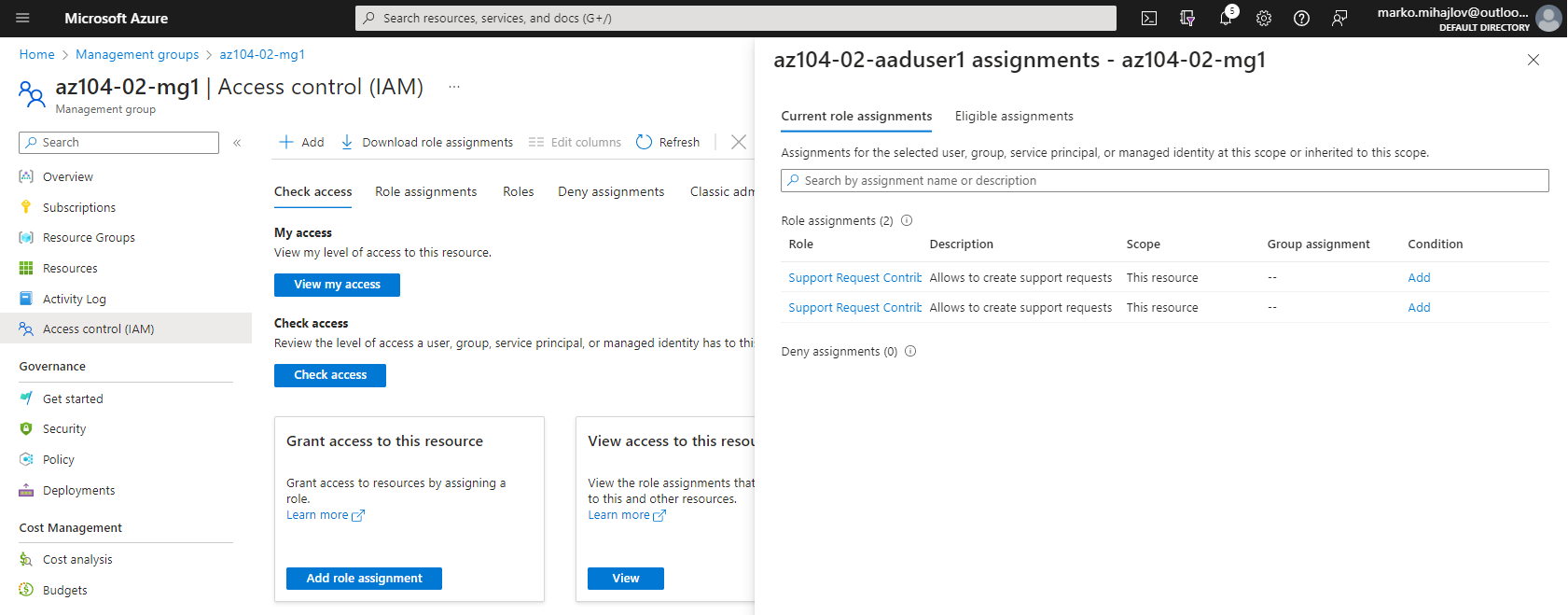
Changing the subscription ID in the role definition JSON file to state the ID of my current subscription Azure former students. Please note that in the following steps of the Lab I had issues viewing the resource groups with the new user that we create for the purposes of this lab - **az104-02-aaduser1. For that reason I created a second template for the custom role in which I entered the subcscription ID of the Azure pass sponsorship which was activated for/on the Azure former students subscription.**

**Although it states that it is a separate subscription I am not able to add it under the newly created management group as it does not appear in the dropdown menu. Therefore I made the conclusion that they are connected in some other nontransparent way.** (Probably it is an alias for the other subscrp.)

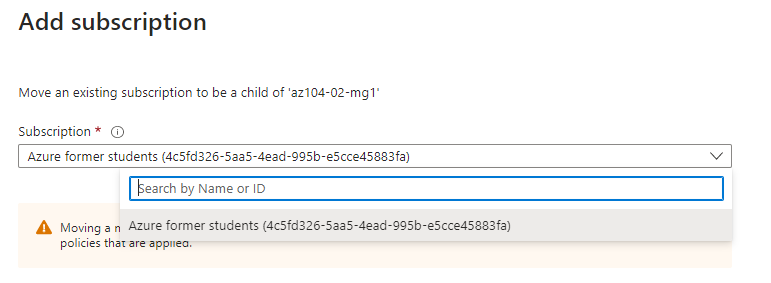
****

After the role assignments are done if I check the role assignment for the user it is stated that both are for az104-02-mg1 and as seen in the screenshot below the azure pass sponsorship cannot be added to az104-02-mg1 ( I assume it is an alias for Azure former students subscription until the sponsorship expires).

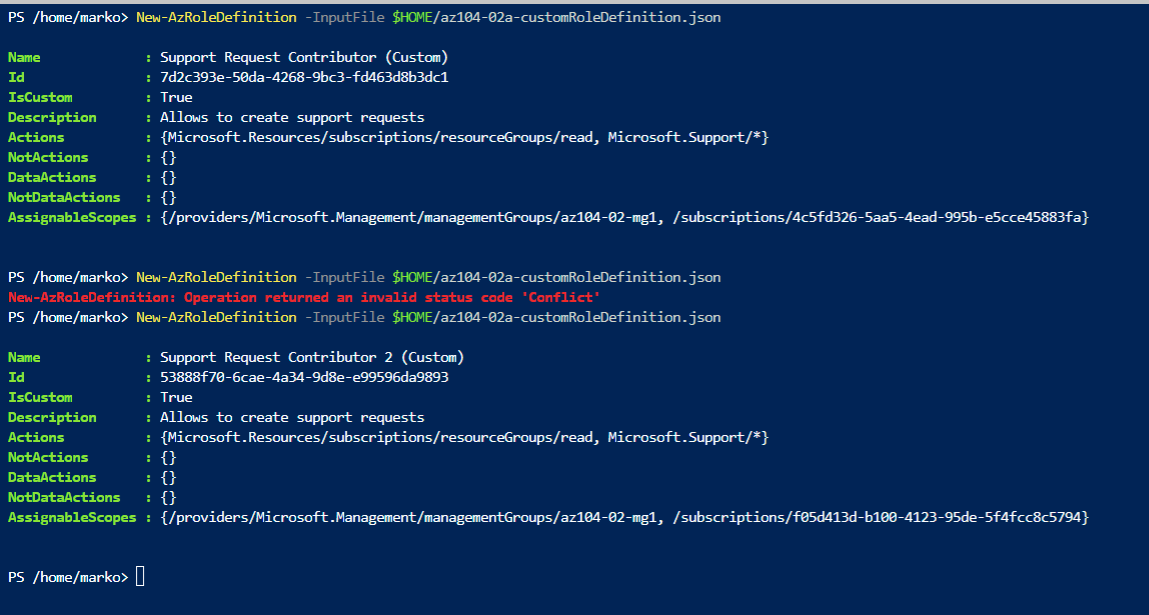
Another way to check access is directly from the Managemeng group Access control blade, check acces:



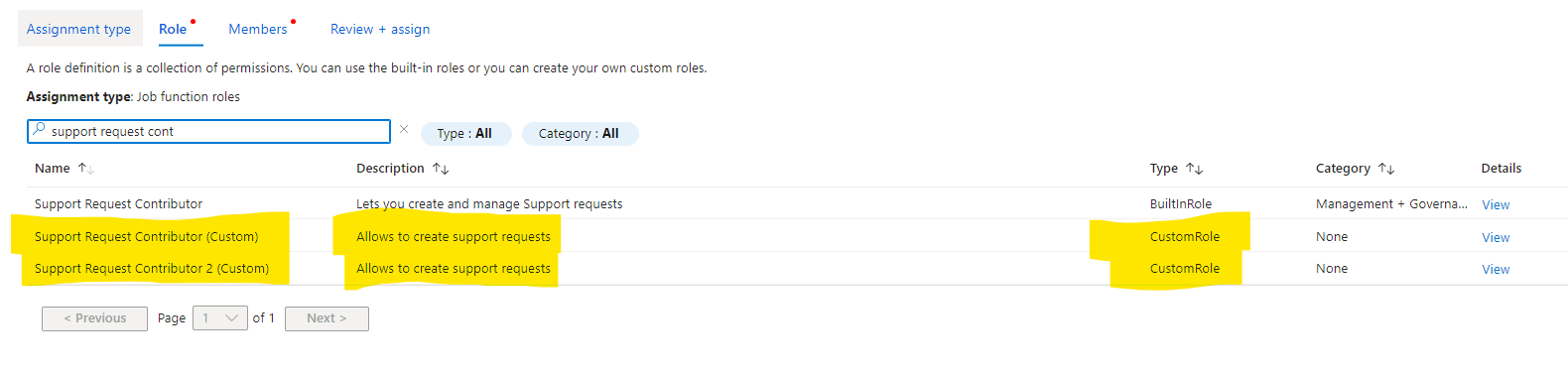


****

**Creating the two custom roles from the definition in the JSON file.**

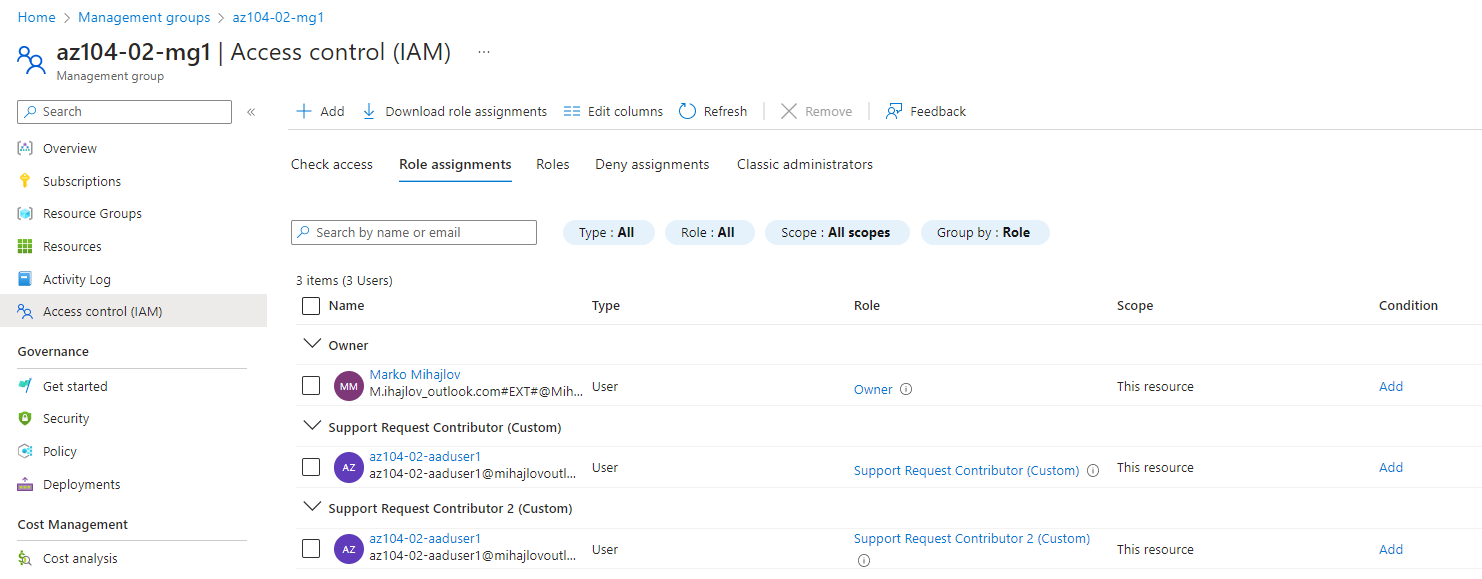
****

**Task 3: Assign RBAC roles**

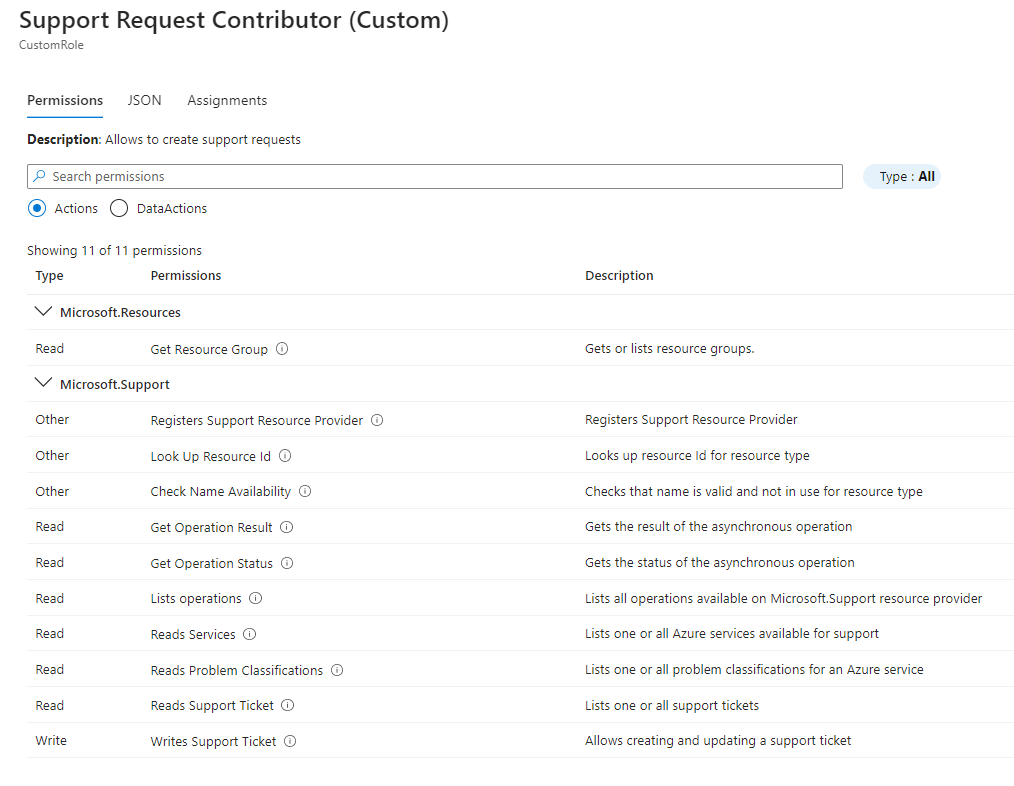
****

**After creating the user az104-02-adduser1 we proceed to create the role assignments for the newly created roles for the user.  
We search for the role needed in question, find the user and finish the role assignment.**

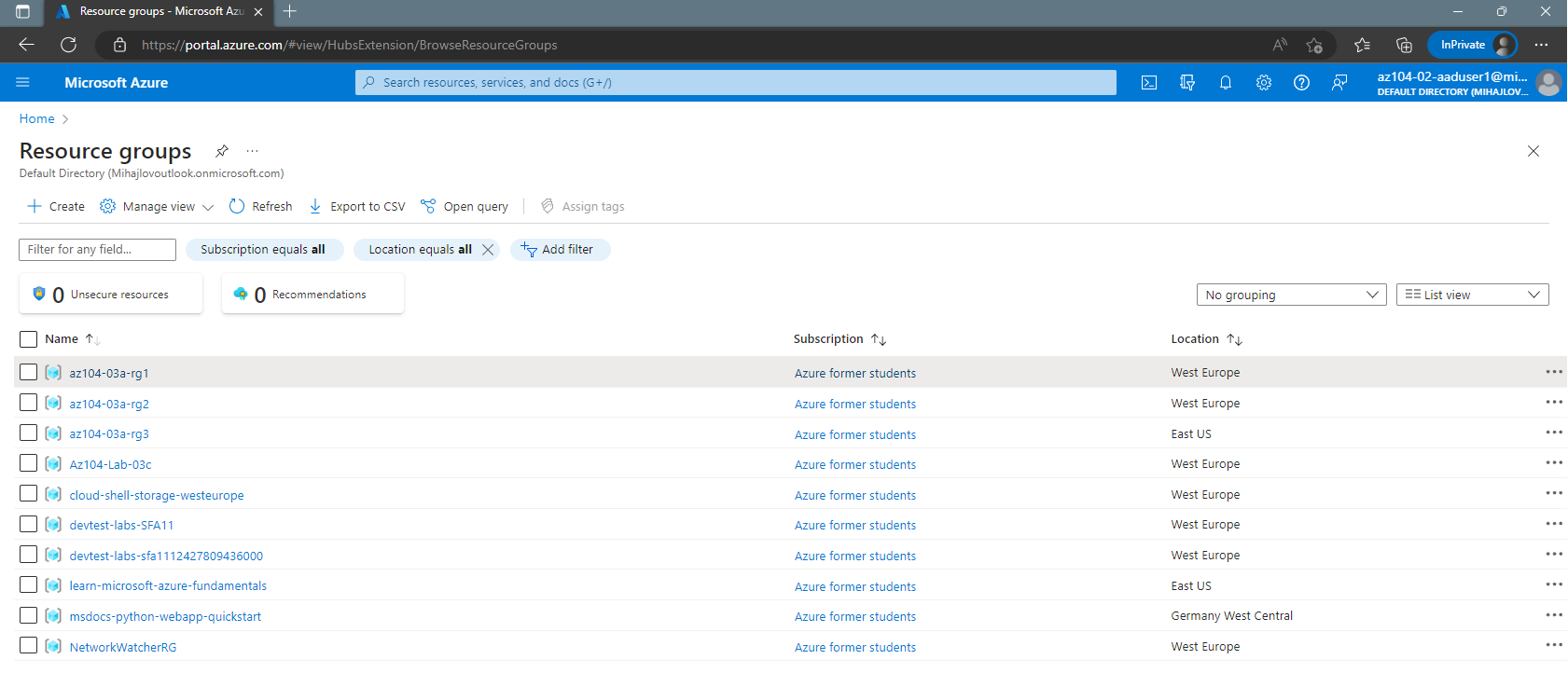
**When checking in the management group IAM blade we can see that the following users have role assignments for the management group: note that these assignments are for the management group and subscriptions/resource groups/ resources below and not if there is another subscription in the root management group. (scope above)  
  
There are 4 scopes - management group, subscription resource group, resource and access can be limited down to the single resource level.**

****

**If we want to check what are all of the operations that the role gives permission for the user to do, we can see in the following place: in the management group blade in the Roles tab if we search for the role we will see the following:**

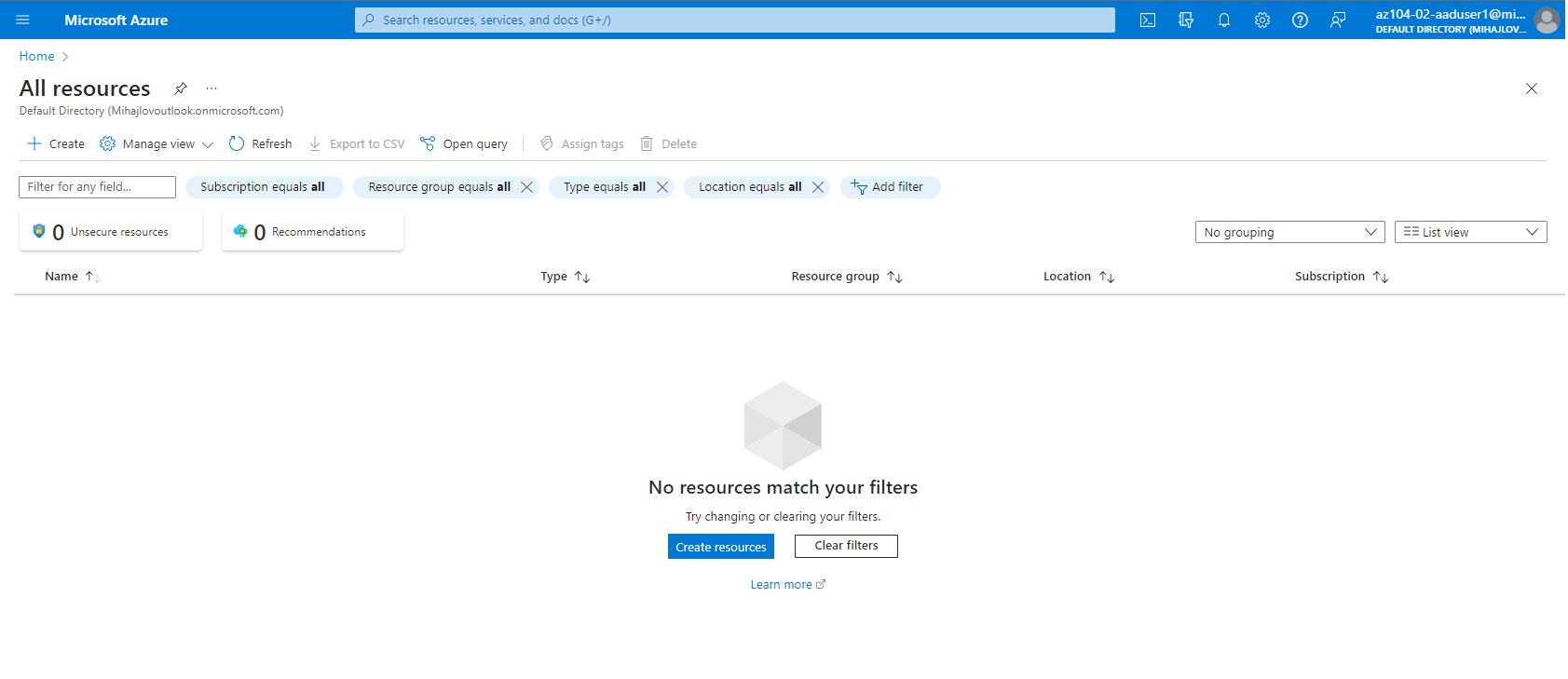
****

**Time to verify that the role assignment is functioning properly:**

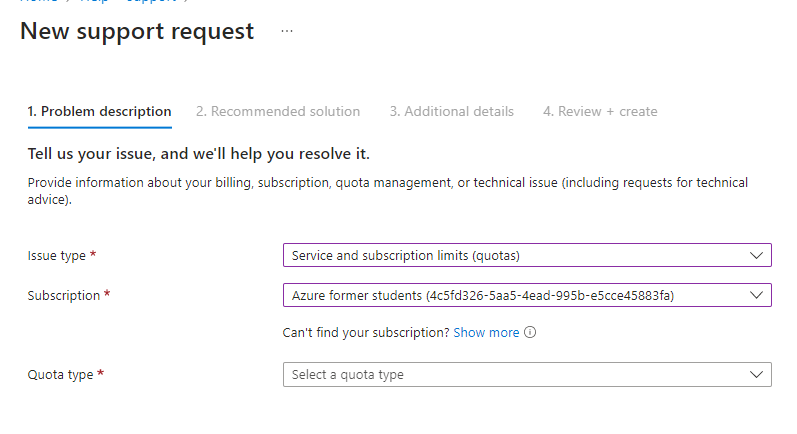
****

**As written in the JSON role definition, the role allows us to read resource groups and ALL (wildcard \* ) to do with the Support section at the Management Group Scope for the subscription/s.**

**(can read resource groups but not resources in the groups themselves)**

****

**Last step checking access in the support section:**

****

**End of File.**