Challenge 1: Azure Governance-Management Groups and RBAC

Introduction

Azure Governance is a collection of concepts and services that are designed to enable management of your various Azure resources at scale. These services provide the ability to organize and structure your subscriptions in a logical way, create and deploy re-usable and Azure native packages of resources, to define, audit and remediate your resources, and more.

Objectives

* Group and organize your subscriptions in a logical hierarchy that support the deployment of other Governance services in a structured way
* Work with RBAC to control access

Lab Requirements

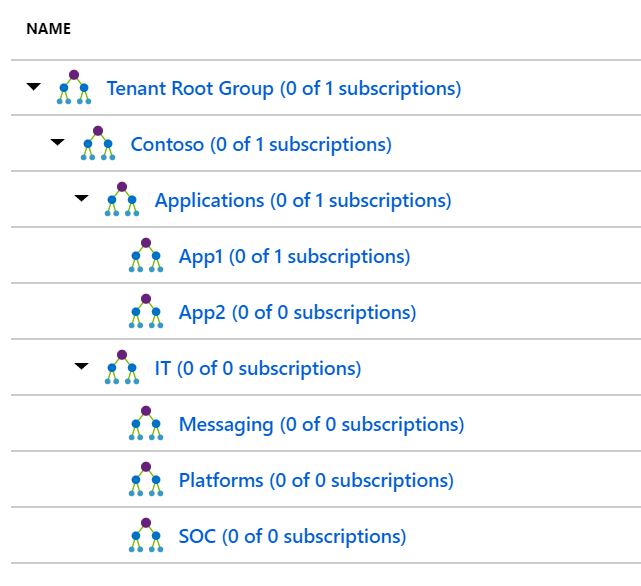
You can perform all steps in this lab from your workstation using the Azure Portal and/or Visual Studio Code.

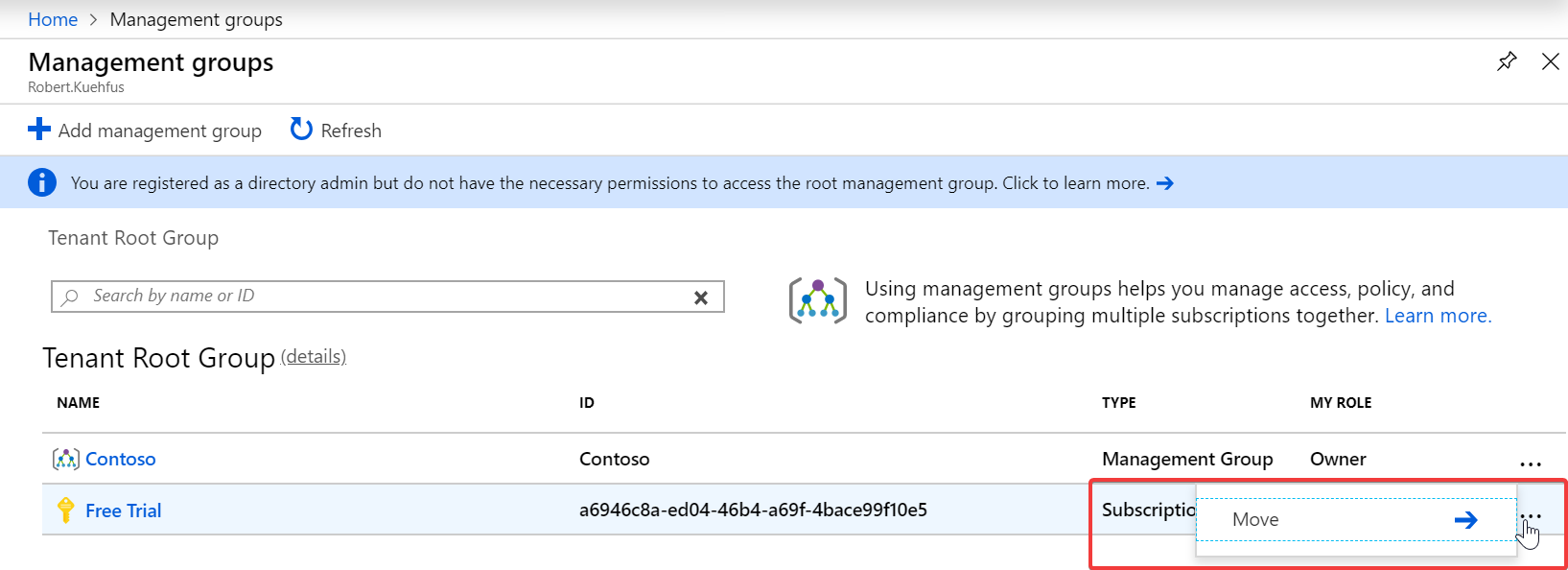
Exercise 1: Create an organization structure with Management Groups

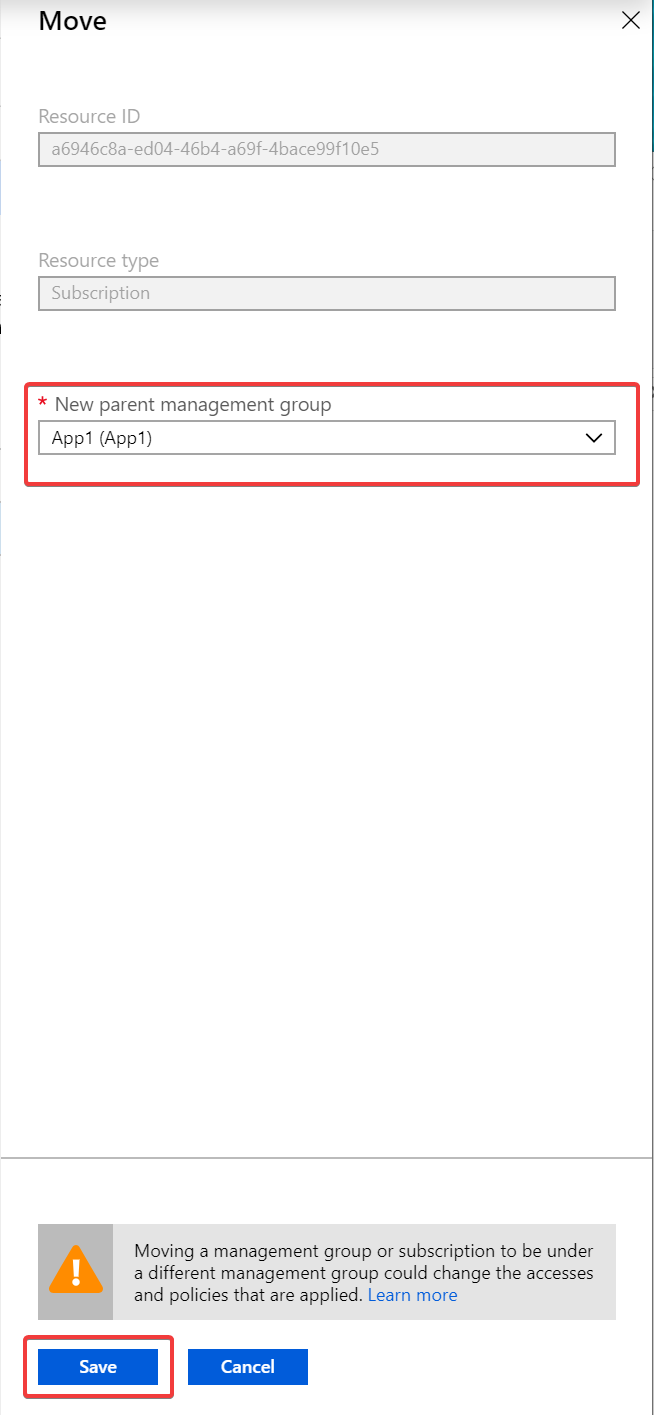
Scenario

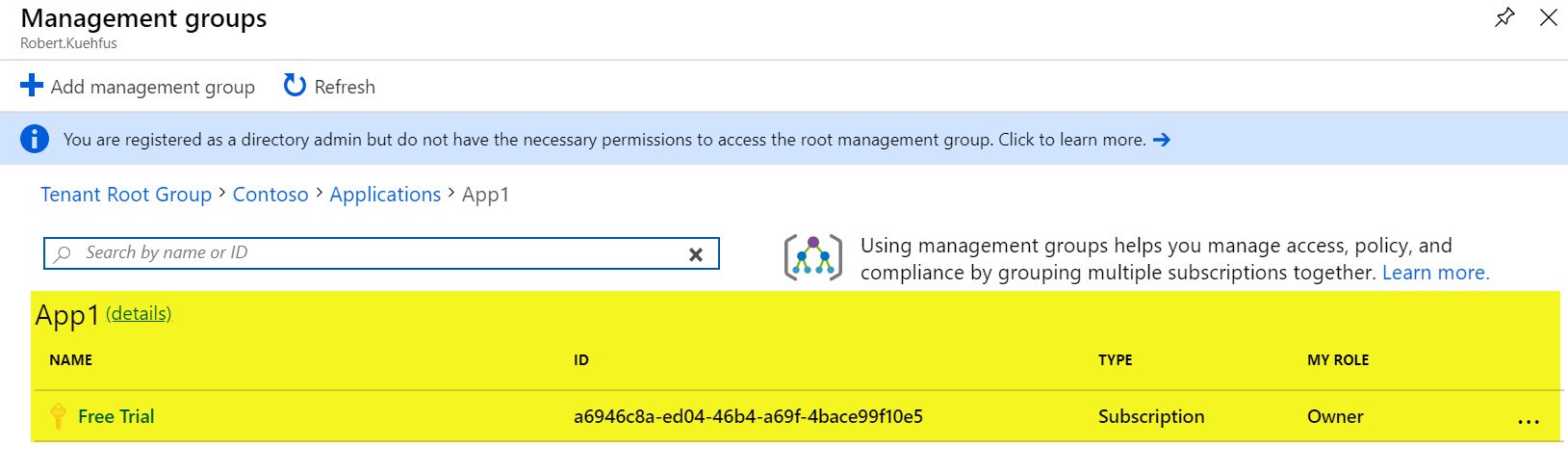
The very first step in implementing a governance strategy in Azure is to create a logical hierarchy in Management Groups

1. Sign in to the Azure Portal using your Azure account
2. Launch the **Management Groups** service in Azure portal by clicking **All services**, then searching for and selecting **Management Groups**.
3. Click **Add Management Group** to create the following structure:

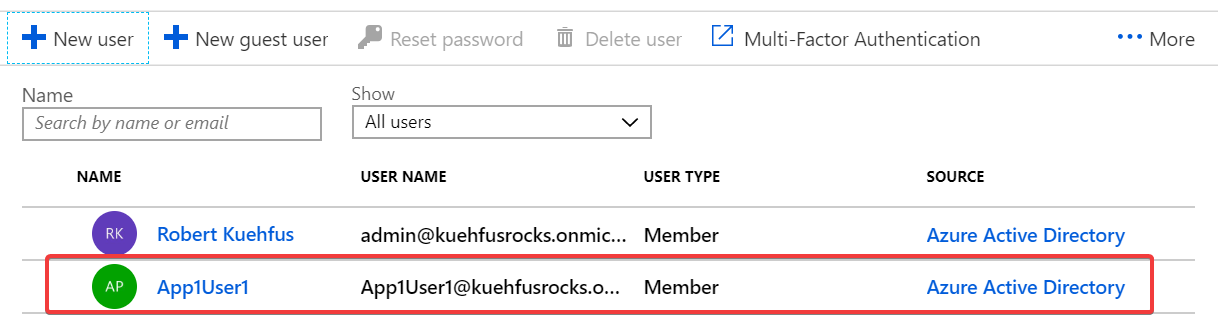
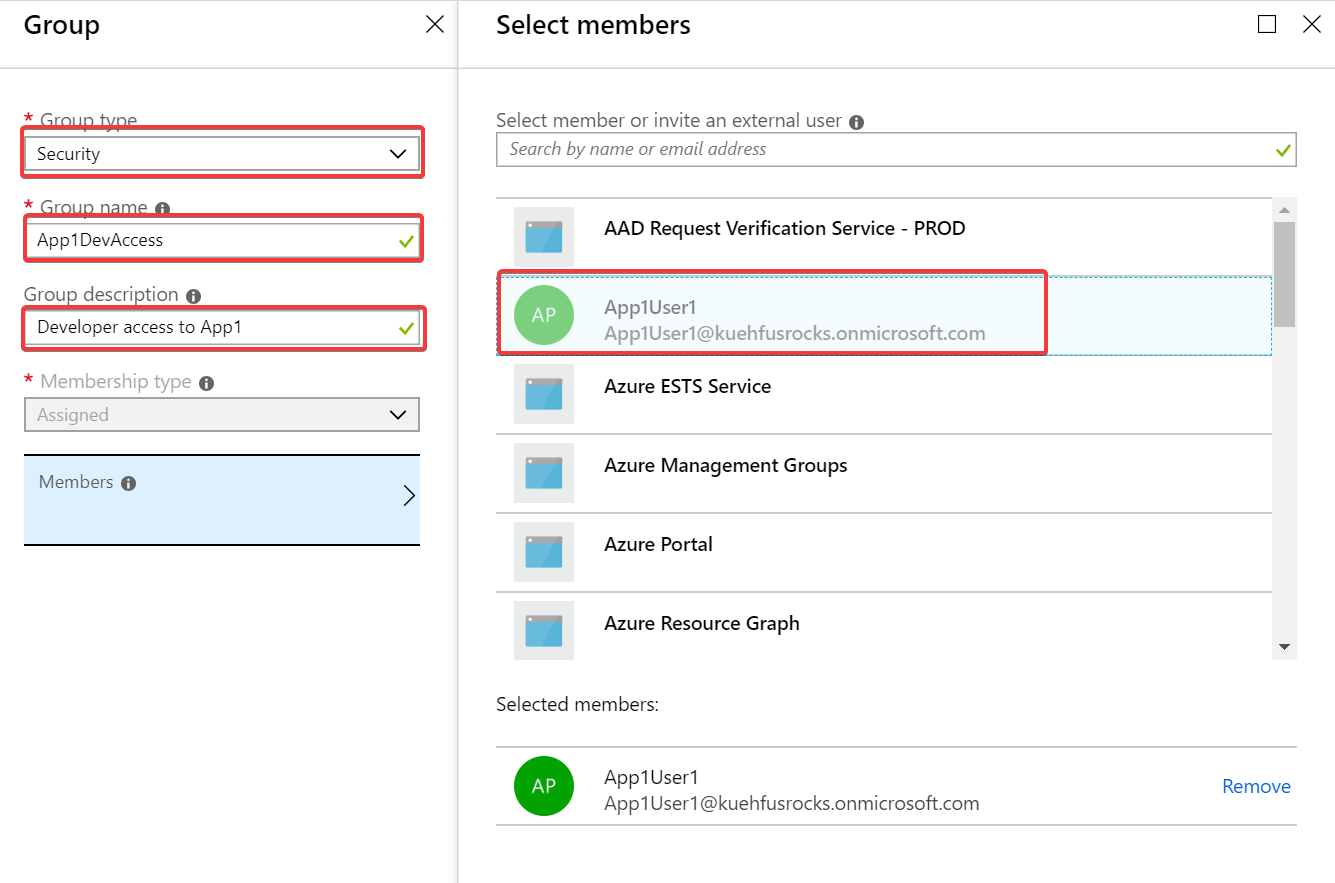
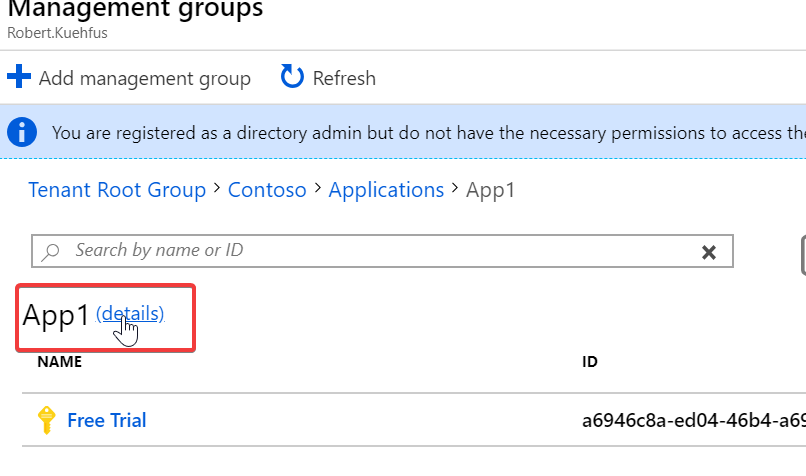
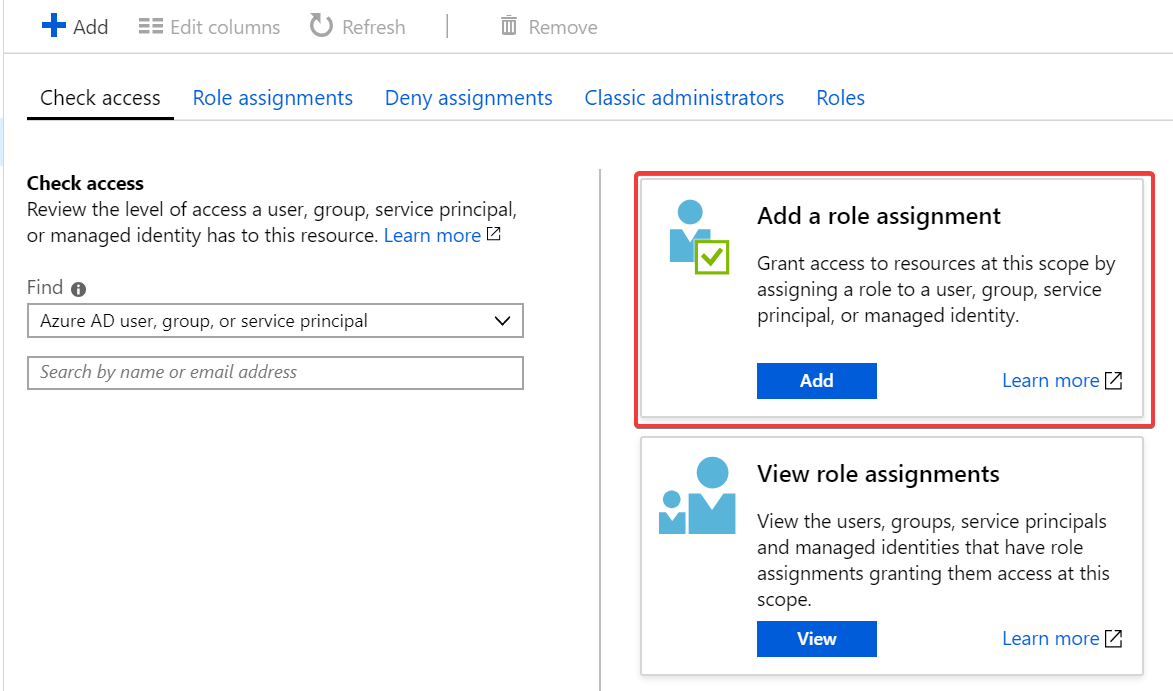
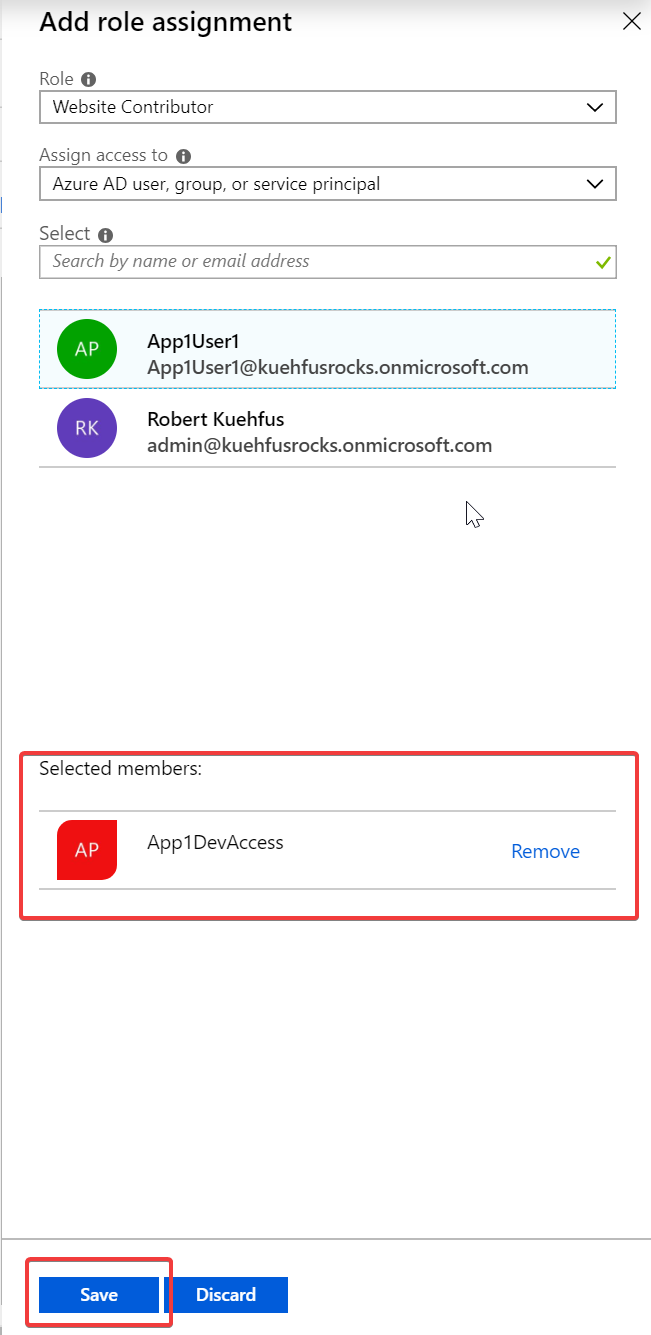
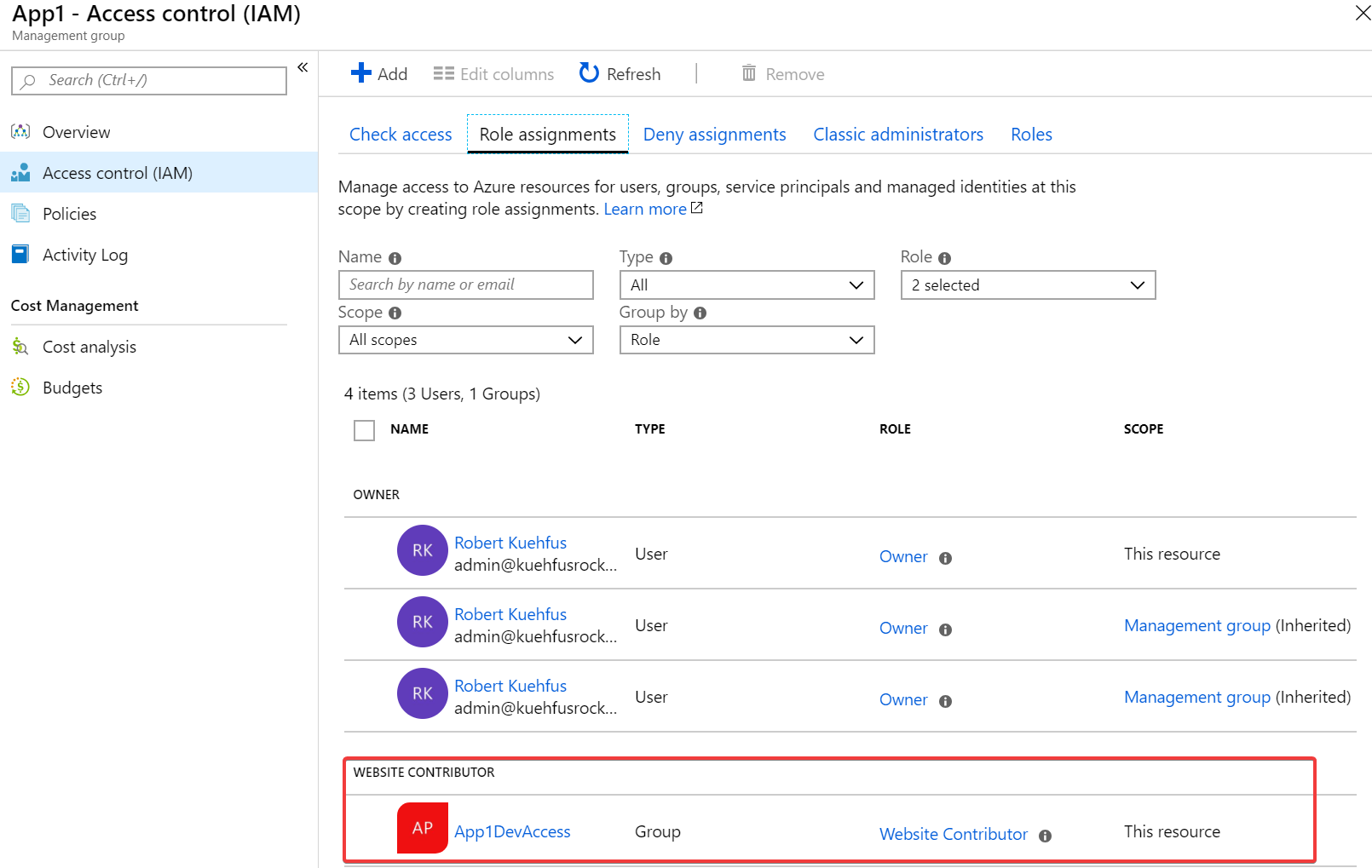
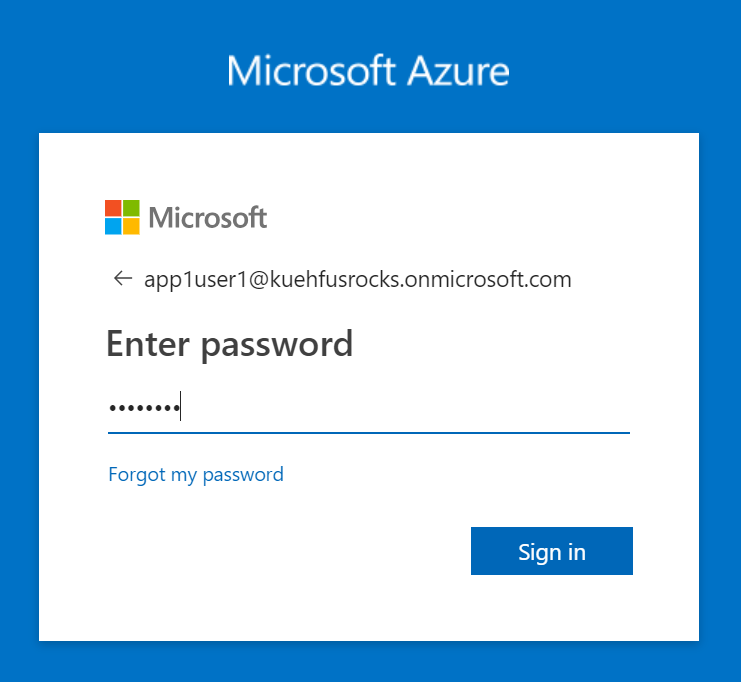
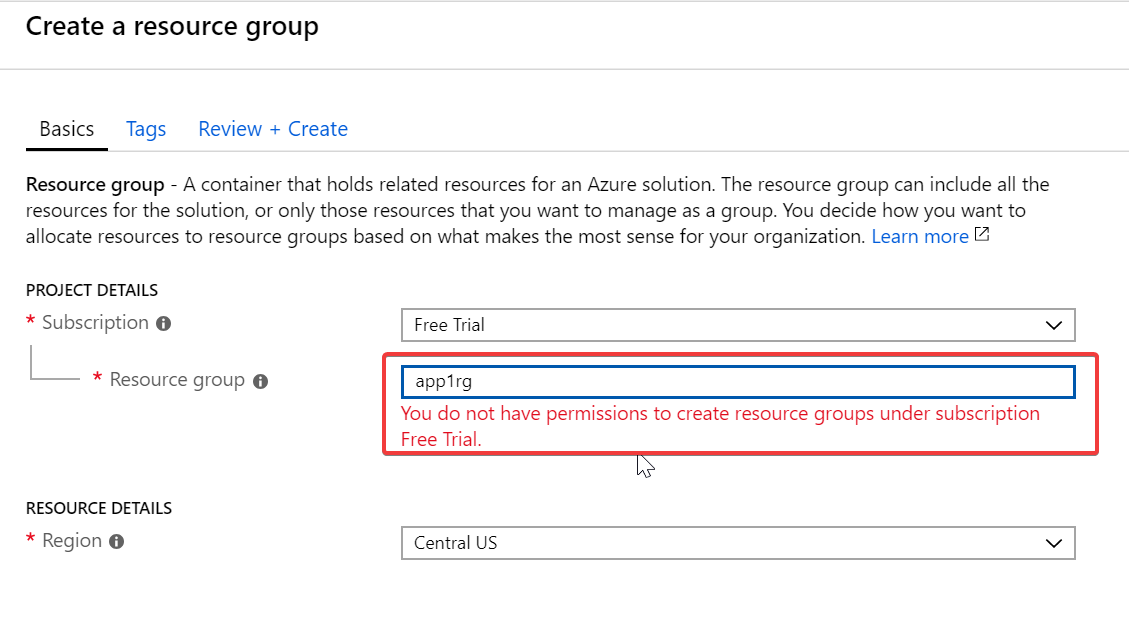
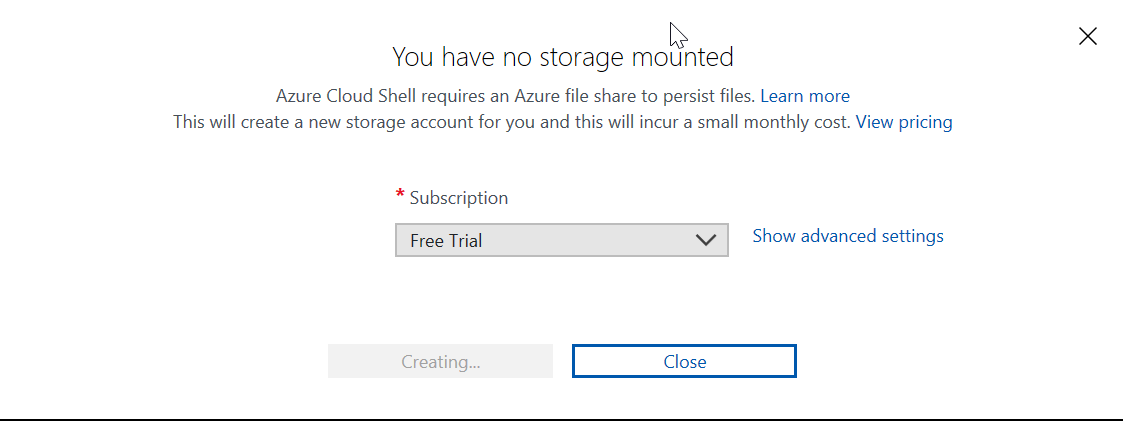


1. Navigate to the **Tenant Root Group**, click the ellipsis next to your subscription, select **Move**
2. Select **App1** and **Save** it.



When you are complete is should look like this -   


 Exercise 2: Create an AD Group and assign permissions to the correct management group

1. Navigate to Azure Active Directory, Users and select New User. Create a user called App1User1. Make sure to make note of the users password.  
   
2. Navigate to Azure Active Directory, Groups and select New Group. Fill out the information similar to below.   
     
   Click Create
3. Grant Website Contributor access to the App1DevAccess group. Navigate to Management Groups and drill down to App1. Click on details.  
   
4. Navigate to Access control (IAM) and select Add under Add a role assignment  
   
5. Under role assignment, select Website Contributor under Role and select you newly created group App1DevAccess  
     
   Click Save.
6. Verify under Role assignments that the Website Contributor has your group assigned.  
   
7. Log into the Azure Portal from a different Tab or browser session using your app1user1@xxx.onmicrosoft.com  
     
   Change your password.
8. Try to create a Resource Group and you should see a message about not having permissions.  
   
9. Create a custom role that grants permissions to create resource groups using the CLI and Azure Cloud Shell. Open the Bash Cloud Shell from the Azure Portal or Visual Studio Code (ctrl+Shift+P). You need to follow the on-screen instructions to create your Bash Cloud Shell for the first time.  
   

From your Cloud Shell, create your custom role by first creating and added the following json to a file called rgcreator.json. The Cloud Shell has both the vi and nano text editor installed for you to use. Note: Make sure to update the AssignableScopes to your Subscription Id.  
{

"Name": "Resource Group Creator",

"IsCustom": true,

"Description": "Can read and create Resource Groups.",

"Actions": [

"Microsoft.Resources/subscriptions/resourceGroups/\*"

],

"NotActions": [

],

"AssignableScopes": [

"/subscriptions/11111111-1111-1111-1111-111111111111"

]

}

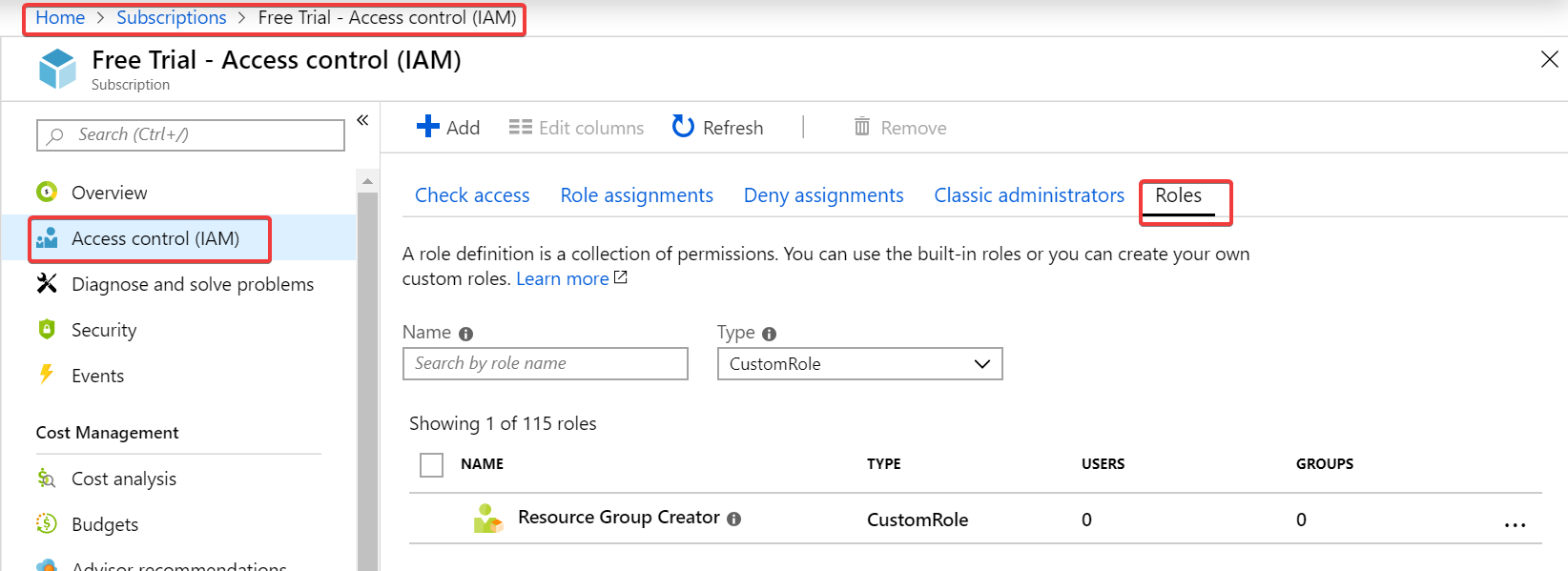
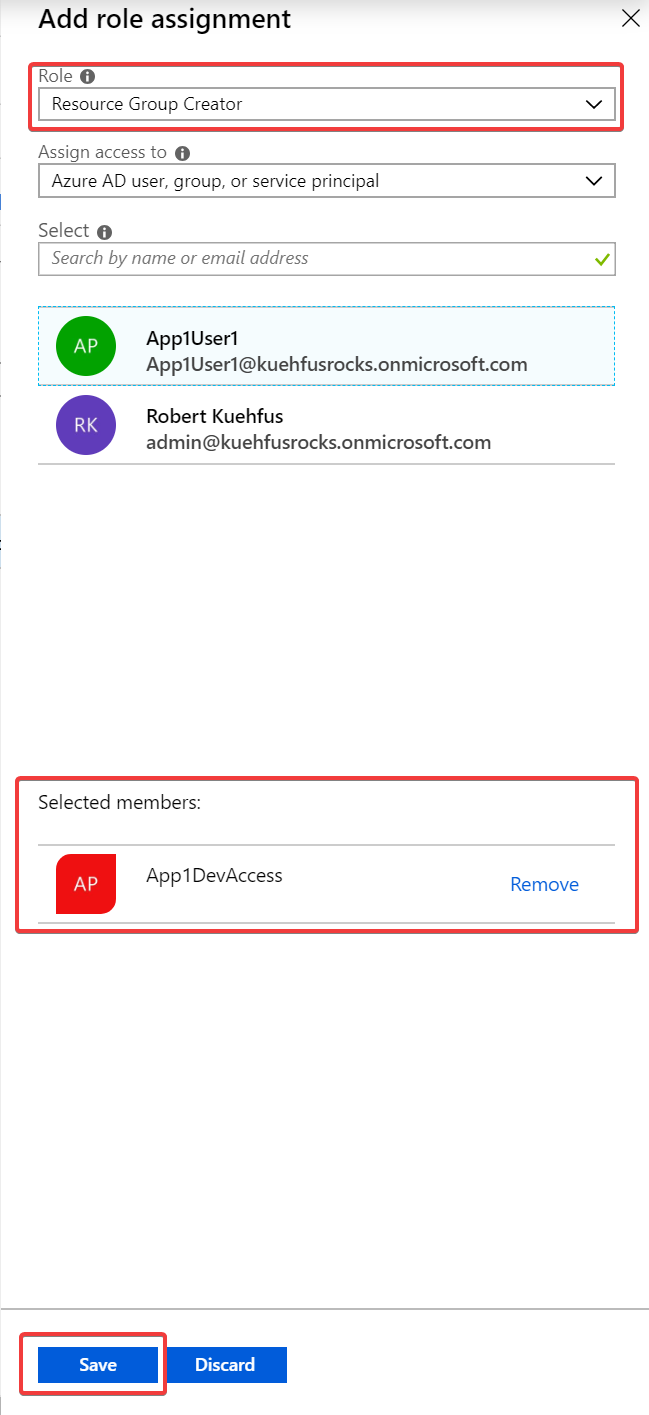
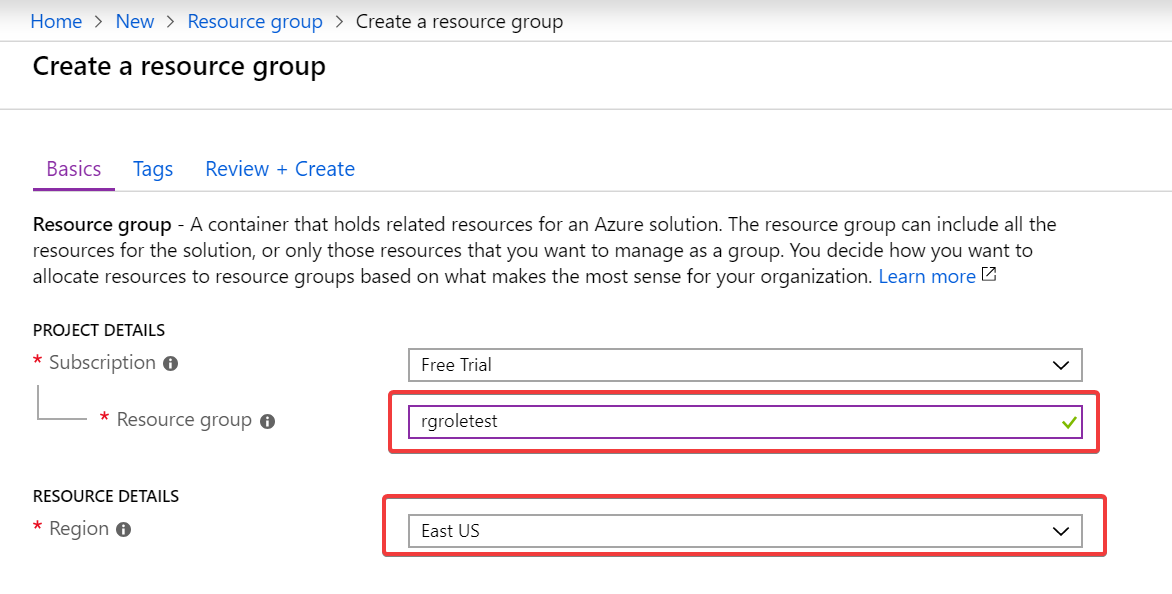
Once you have created the rgcreator.json file run the following command:

#Create custom Role

az role definition create --role-definition ./rgcreator.json

#List the new custom role

az role definition list --name "Resource Group Creator"

1. Currently Management Groups do not support creating custom roles from the Management Group level. Our custom role was created at the subscription level. From your admin account, navigate to Subscriptions and click into your Subscription (Free Trial). Select Access control (IAM) and Roles.  
     
   Click on Add
2. Select the Resource Group Creator Role and the App1DevAccess Group  
     
   Click Save
3. Log into the Azure Portal as your App1User1 user and try to create a resource group.  
     
   Click Review + Create, Create
4. Navigate to the Resource Group view and verify the resource group has been created  
   