ENPM665 – Identity and Access Management Exercises

Version 2.2 – September 21st 2022

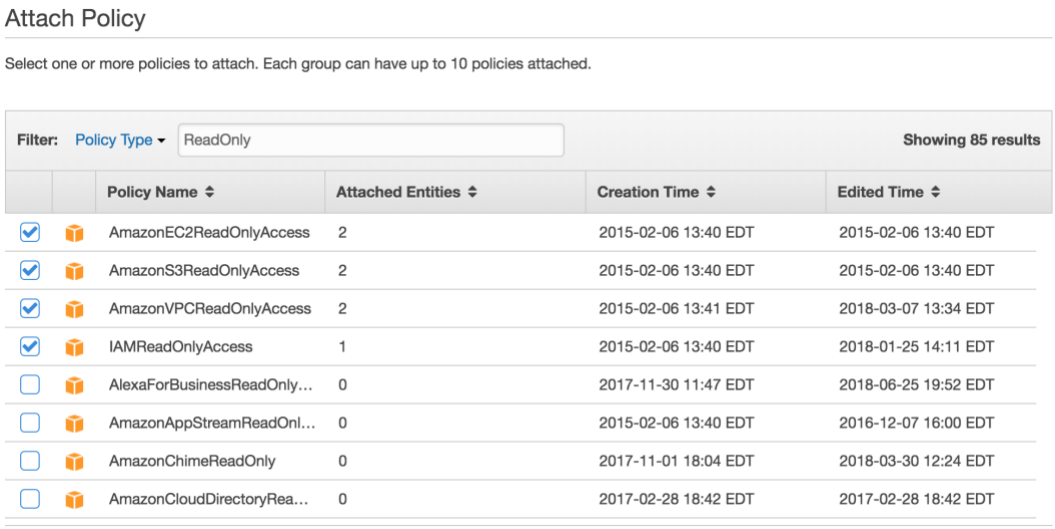
AWS IAM Exercises

We'll experiment with a few different parts of AWS IAM in this exercise.

Create a group and assign permissions to it

1. Login to the AWS Console – https://aws.amazon.com/
2. In the console navigate to the **IAM** Service
3. Select **Groups**
4. Click "**Create New Group**"
5. Give it a name, I will use "**ENPM809J-ReadOnly**" then click "**Next Step**"
6. On the Attach Policy page click the Filter and enter "**readonly**"
7. Select some of the read only access policies like "**AmazonEC2ReadOnlyAccess**", "**AmazonS3ReadOnlyAccess**", "**IAMReadOnlyAccess**"

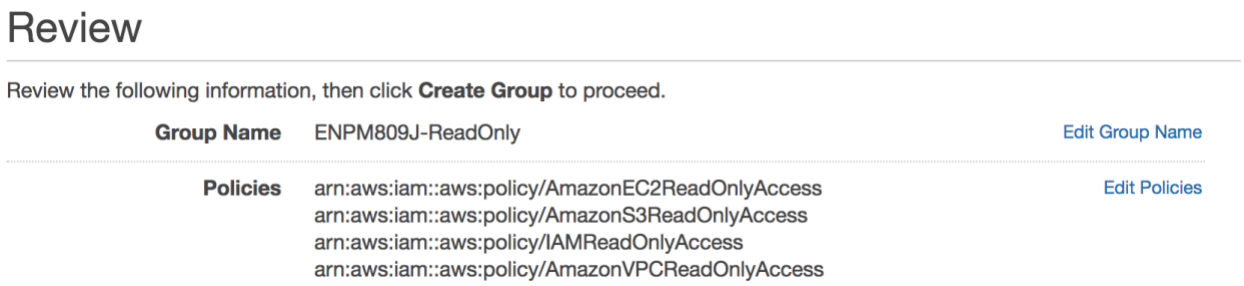
   Note: Ensure that "**AmazonEC2ReadOnlyAccess**" is selected, we'll need it for some examples below.



Policy Name	Attached Entities	Creation Time	Edited Time
AmazonEC2ReadOnlyAccess	2	2015-02-06 13:40 EDT	2015-02-06 13:40 EDT
AmazonS3ReadOnlyAccess	2	2015-02-06 13:40 EDT	2015-02-06 13:40 EDT
AmazonVPCReadOnlyAccess	2	2015-02-06 13:41 EDT	2018-03-07 13:34 EDT
IAMReadOnlyAccess	1	2015-02-06 13:40 EDT	2018-01-25 14:11 EDT
AlexaForBusinessReadOnly...	0	2017-11-30 11:47 EDT	2018-06-25 19:52 EDT
AmazonAppStreamReadOnl...	0	2015-02-06 13:40 EDT	2016-12-07 16:00 EDT
AmazonChimeReadOnly	0	2017-11-01 18:04 EDT	2018-03-30 12:24 EDT
AmazonCloudDirectoryRea...	0	2017-02-28 18:42 EDT	2017-02-28 18:42 EDT

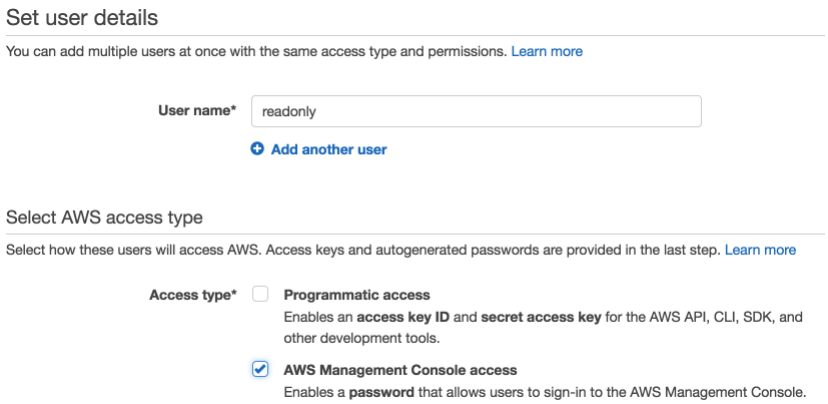
8. Click "**Next Step**"

9. Review and then click “**Create Group**”

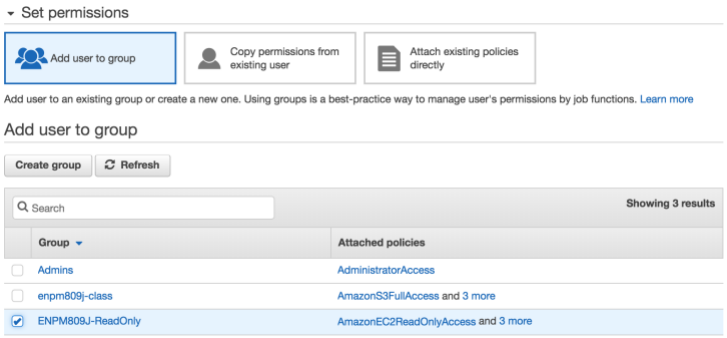


Create a user in that group

1. Select “**Users**”
2. Click the “**Add user**” button
3. Select a user name, I’ll use “**readonly**”
4. Click “**AWS Management Console access**” for the access type.



5. You can scroll down and select a password for the user, or use an autogenerated one.
6. Click “**Next: Permissions**”
7. “Add user to group” is selected by default, click the checkbox next to the group you created above (“**ENPM809J-RealOnly**” is what I used)

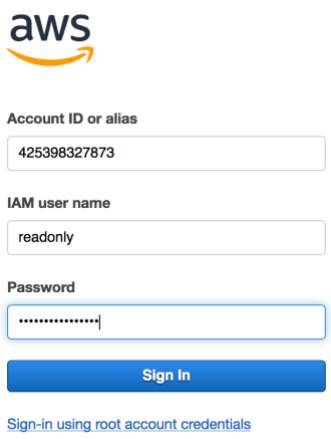


8. Click "**Next: Tags**"
9. Click "**Next: Review**"
10. Review and click "**Create user**"
11. The next page will show you the custom URL for your AWS account for logging in with your newly created user. It will look like: https://425398327873.signin.aws.amazon.com/console

    You'll also see the option to view the automatically generated password for the new user you created. You can use that password or create a new password for the user by clicking their name in the user list, clicking the "Security Credentials" tab, and then the "Manage password" link to change the password.

Login to your account's customized URL with the newly created account

1. In either a different web browser, or an Incognito/Private browsing tab login to the custom URL for your AWS account. User name and password will be the ones from the steps completed above. (ex: User = "**readonly**")

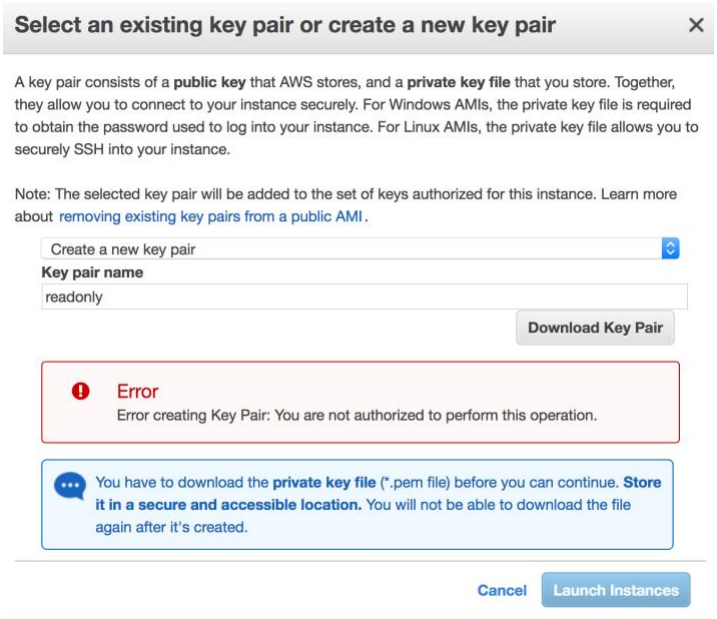


2. You will most likely need to select a new password. Follow the instructions on the page to do so.

Attempt to start up an EC2 instance

1. In the AWS Services select **EC2**
2. Click the "**Launch Instance**" button
3. Select any Amazon Machine Image you like. I'll use the following:
    - AMI: "**Amazon Linux 2 AMI (HVM), SSD Volume Type**"
    - Instance Type: **t2.micro**

4. Click "**Review and Launch**"
5. Click "**Launch**"
6. You'll be asked to create a key pair for logging in. Select "**Create a new key pair**" and give it a name (Ex: "**readonly**")
7. Click "**Download Key Pair**" What happens? You should see an error message like this:

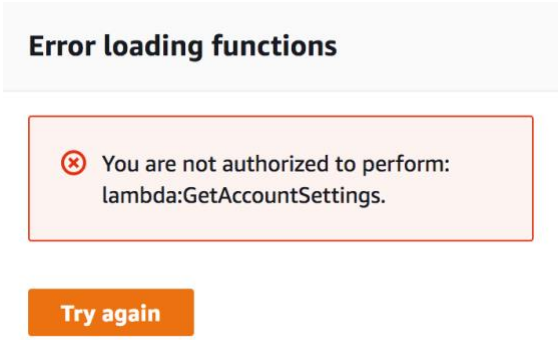


Why does this happen? (Because you only have "read only" access to EC2!)

8. **Cancel** out of the window.
9. **Cancel** again to get out of the EC2 launch wizard.

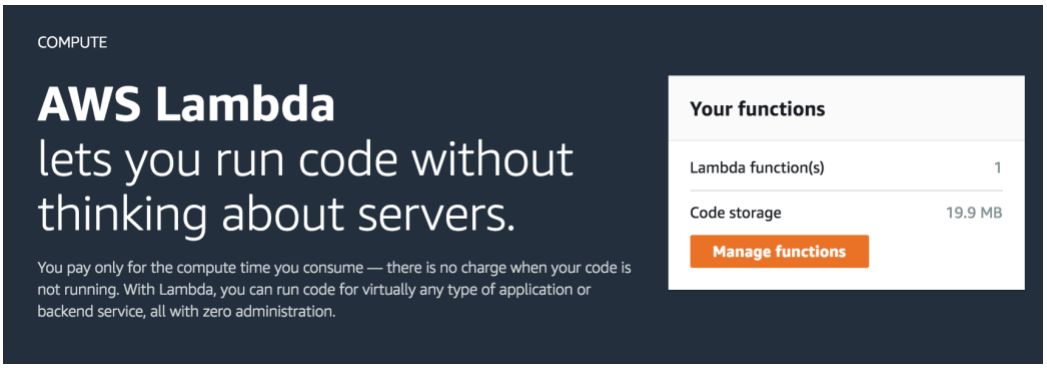
Attempt to access an AWS Service we do not have read only access to

1. In the AWS Console under Services select "**Lambda**"
2. You should get a splash page for Lambda that describes that it is and an error message.



3. Do the same thing with an account that has access to Lambda, you'll see the splash page but instead of an error message you'll get a listing of any Lambda functions you have.

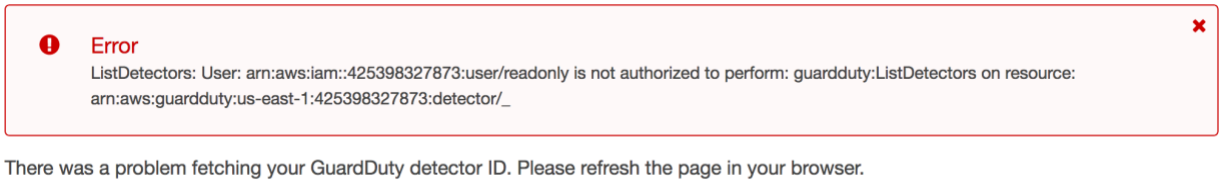
   Ex:



4. Do the same thing with other AWS Services.

   Example – GuardDuty with full access:

   Example – GuardDuty with "readonly" account :



(Optional) Further exercises:

- With an account that has access to create and run EC2 instances start an EC2 instance. Then with the "readonly" account review details of the EC2 instance. Attempt to stop it. What happens?

- With an account that has access to create a VPC, create a VPC. Then with the "readonly" account attempt to delete it or modify it. What happens?

- With the account that has access to change IAM permissions add and remove various permissions for the “readonly” user and/or “ENPM809J-ReadOnly” group. Then attempt to access those services with the readonly user. You can experiment to see how fast changes take place as well as what addition things you can/can not see after the changes are made.

Azure IAM Exercises

Login to the Azure Portal - https://portal.azure.com/

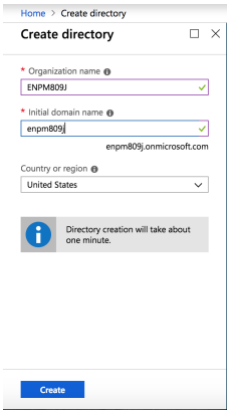
Create Azure AD environment

Create a new Azure AD environment by doing the following:

1. In a web browser navigate to https://portal.azure.com/#create/Microsoft.AzureActiveDirectory and login if needed.
2. Enter the organization name (ex. “**ENPM809J**”)
3. Select an initial domain name (ex. “**enpm809j**”. These need to be unique to I’d recommend you use something like the course name + your Directory ID “**enpm809jkts**”)

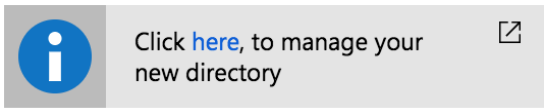
   Note: This will create a hostname of enpm809j< your Directory ID>.onmicrosoft.com (ex: **enpm809jkts.onmicrosoft.com**”)

4. Click “**Create**”



5. Wait for the directory to be created. It may take a few minutes. Once completed you’ll get a popup saying that creation was successful.

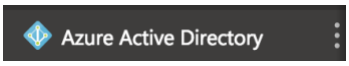
6. Look for the message that says “Click here, to manage your new directory” and click “**here**”



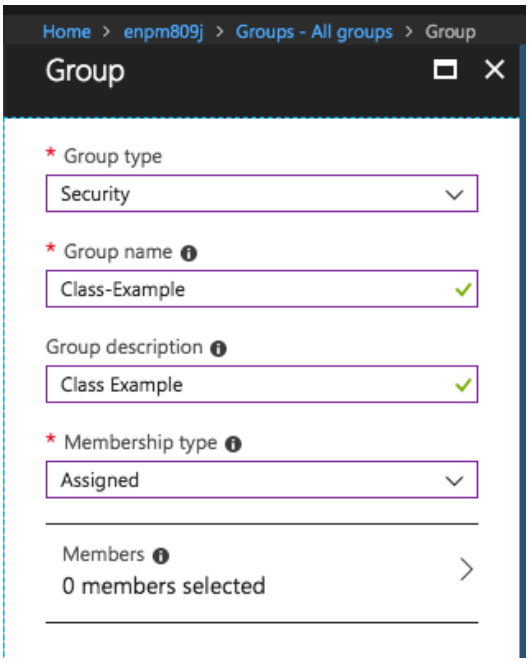
7. This will take you to the Azure AD portal for your newly created Azure Active Directory Domain.

Create a Group in Azure

1. In the Azure portal, in the left-hand menu click the “**Azure Active Directory**” icon.



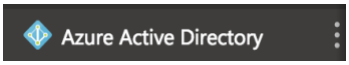
2. Under Manager select “**Groups**”
3. Click the “**New Group**” button
4. Use the following settings:
    a. Group type – **Security**
    b. Group name – **Class-Example**
    c. Group description – (Whatever you like, you can leave blank)
    d. Membership type – **Assigned**



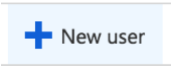
5. Click “**Create**”

Create a User in Azure AD

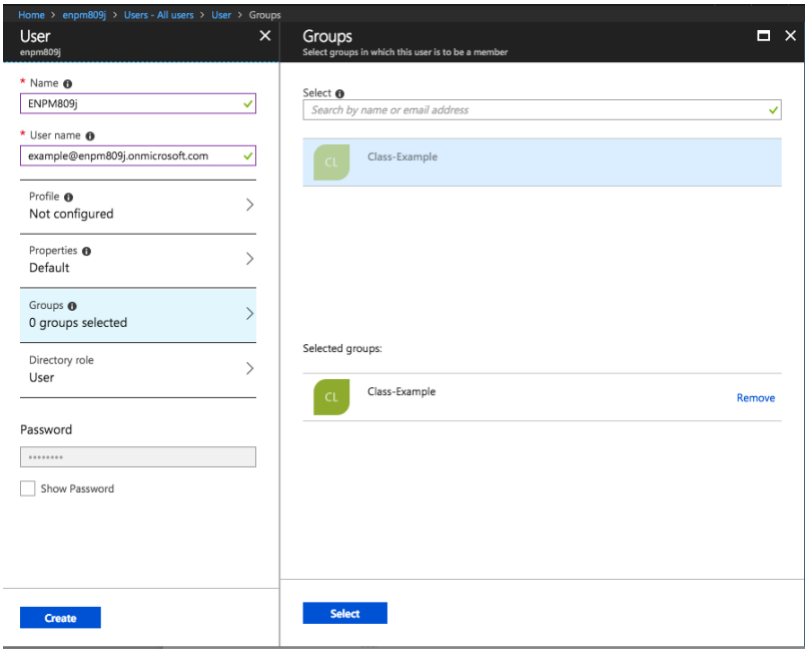
1. In the Azure portal, in the left-hand menu click the "**Azure Active Directory**" icon.



2. Under Manage click "**Users**"
3. Click the "**New user**" icon



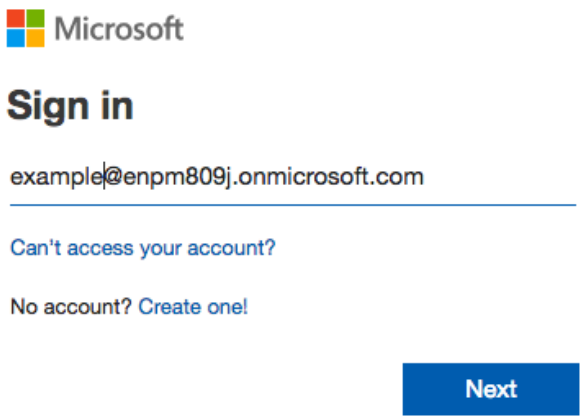
4. For the user's Name enter whatever you want.
5. For the user name use whatever you'd like. (ex: "**example@enpm809j.onmicrosoft.com**" – replace "enpm809j with what your Azure AD domain is. **Note**: you MUST enter the Azure AD name + ".onmicrosoft.com")
6. Click "**Groups**" and add the user to the "**Class-Example**" group
7. Memorize/Copy the password that is generated or enter your own for this account.
8. Click "**Create**"



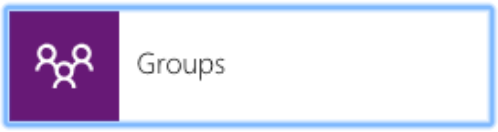
Test the Azure AD User login

The user you created can login to their account and Microsoft's MyApps portal. This would be their interface to access Azure and other resources.

1. In a different web browser or an incognito/private browsing tab open http://myapps.microsoft.com
2. For the user name enter the user name you created above (ex: example@enpm809j.onmicrosoft.com)



3. Enter the password you saved from above.
4. You'll be taken to the MyApps page, click the groups link on the right side



5. You should see a list of the groups that sample user is in.