

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.

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type ▾		ReadOnly		Showing 85 results	
	Policy Name ↕	Attached Entities ↕	Creation Time ↕	Edited Time ↕	
<input checked="" type="checkbox"/>	 AmazonEC2ReadOnlyAccess	2	2015-02-06 13:40 EDT	2015-02-06 13:40 EDT	
<input checked="" type="checkbox"/>	 AmazonS3ReadOnlyAccess	2	2015-02-06 13:40 EDT	2015-02-06 13:40 EDT	
<input checked="" type="checkbox"/>	 AmazonVPCReadOnlyAccess	2	2015-02-06 13:41 EDT	2018-03-07 13:34 EDT	
<input checked="" type="checkbox"/>	 IAMReadOnlyAccess	1	2015-02-06 13:40 EDT	2018-01-25 14:11 EDT	
<input type="checkbox"/>	 AlexaForBusinessReadOnly...	0	2017-11-30 11:47 EDT	2018-06-25 19:52 EDT	
<input type="checkbox"/>	 AmazonAppStreamReadOnl...	0	2015-02-06 13:40 EDT	2016-12-07 16:00 EDT	
<input type="checkbox"/>	 AmazonChimeReadOnly	0	2017-11-01 18:04 EDT	2018-03-30 12:24 EDT	
<input type="checkbox"/>	 AmazonCloudDirectoryRea...	0	2017-02-28 18:42 EDT	2017-02-28 18:42 EDT	

8. Click **"Next Step"**

- Review and then click **“Create Group”**

Review

Review the following information, then click **Create Group** to proceed.

Group Name	ENPM809J-ReadOnly	Edit Group Name
Policies	arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess arn:aws:iam::aws:policy/IAMReadOnlyAccess arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess	Edit Policies

Create a user in that group

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

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type* ☐ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

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

▼ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user’s permissions by job functions. [Learn more](#)

Add user to group

Create group

Refresh

Search

Showing 3 results

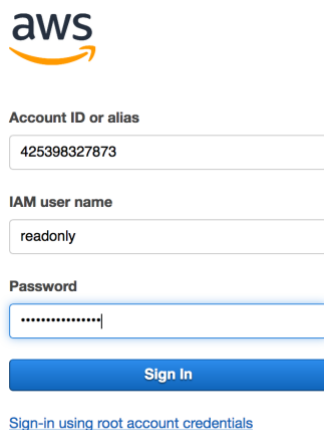
Group	Attached policies
<input type="checkbox"/> Admins	AdministratorAccess
<input type="checkbox"/> enpm809j-class	AmazonS3FullAccess and 3 more
<input checked="" type="checkbox"/> ENPM809J-ReadOnly	AmazonEC2ReadOnlyAccess and 3 more

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”**)



The screenshot shows the AWS login interface. At the top is the AWS logo. Below it, the text "Account ID or alias" is followed by a text input field containing "425398327873". Below that, the text "IAM user name" is followed by a text input field containing "readonly". Below that, the text "Password" is followed by a password input field with masked characters. A blue "Sign In" button is at the bottom. Below the button is a link that says "Sign-in using root account credentials".

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:

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name

readonly

Download Key Pair

Error

Error creating Key Pair: You are not authorized to perform this operation.

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

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.

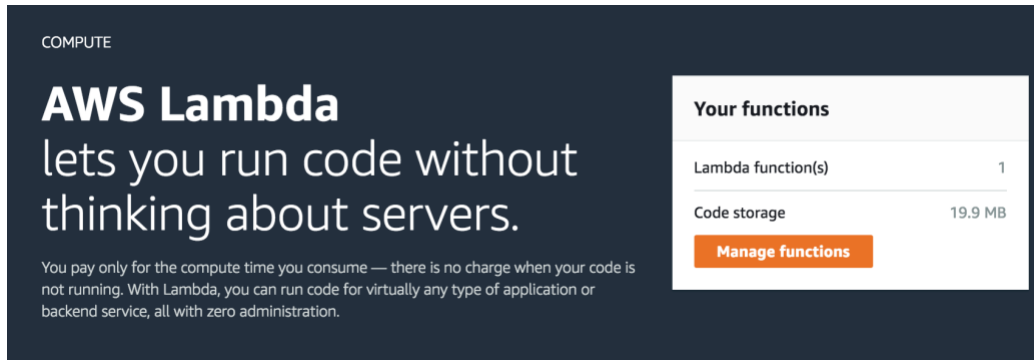
Error loading functions

You are not authorized to perform:
lambda:GetAccountSettings.

Try again

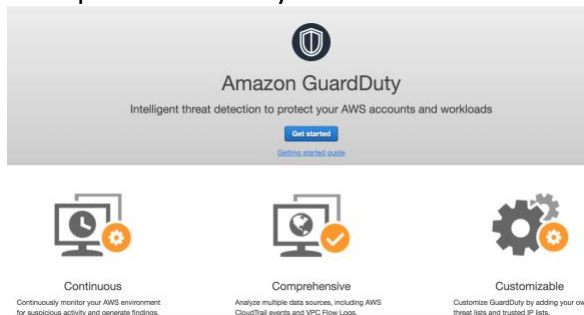
3. Do the same thing with an account that has access to Lambda, you'll see the splash page but instead of an error message you'll get a listing of any Lambda functions you have.

Ex:

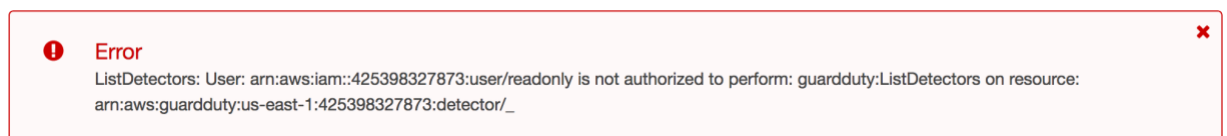


4. Do the same thing with other AWS Services.

Example – GuardDuty with full access:



Example – GuardDuty with “readonly” account :



There was a problem fetching your GuardDuty detector ID. Please refresh the page in your browser.

(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/>

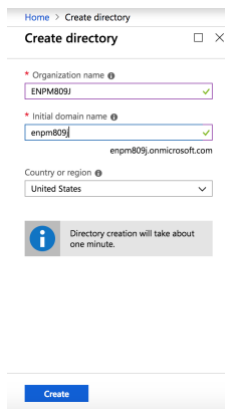
Create Azure AD environment

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 “enpm809jks”)


Note: This will create a hostname of enpm809j< your Directory ID>.onmicrosoft.com (ex: enpm809jks.onmicrosoft.com”)


4. Click “Create”





Home > Create directory

Create directory

* Organization name 
ENPM809J ✓

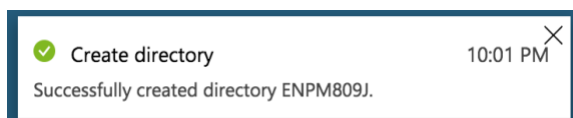
* Initial domain name 
enpm809j ✓
enpm809j.onmicrosoft.com

Country or region 
United States

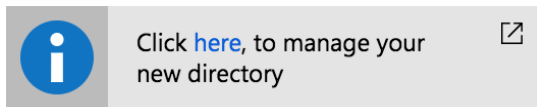
 Directory creation will take about one minute.

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.



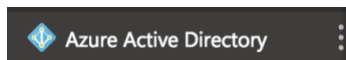
6. Look for the message that says “Click here, to manage your new directory” and click “here”



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.



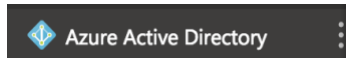
2. Under Manager select “**Groups**”
3. Click the “**New Group**” button
4. Use the following settings:
 - a. Group type – **Security**
 - b. Group name – **Class-Example**
 - c. Group description – (Whatever you like, you can leave blank)
 - d. Membership type – **Assigned**

A screenshot of the Azure AD 'New Group' form. The breadcrumb trail at the top reads 'Home > enpm809j > Groups - All groups > Group'. The title bar says 'Group' with a close button. The form has four required fields, each marked with a red asterisk: 'Group type' is a dropdown menu with 'Security' selected; 'Group name' is a text box with 'Class-Example' and a green checkmark; 'Group description' is a text box with 'Class Example' and a green checkmark; 'Membership type' is a dropdown menu with 'Assigned' selected. Below these fields is a 'Members' section with a text box showing '0 members selected' and a right-pointing arrow.

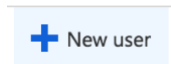
5. Click “**Create**”

Create a User in Azure AD

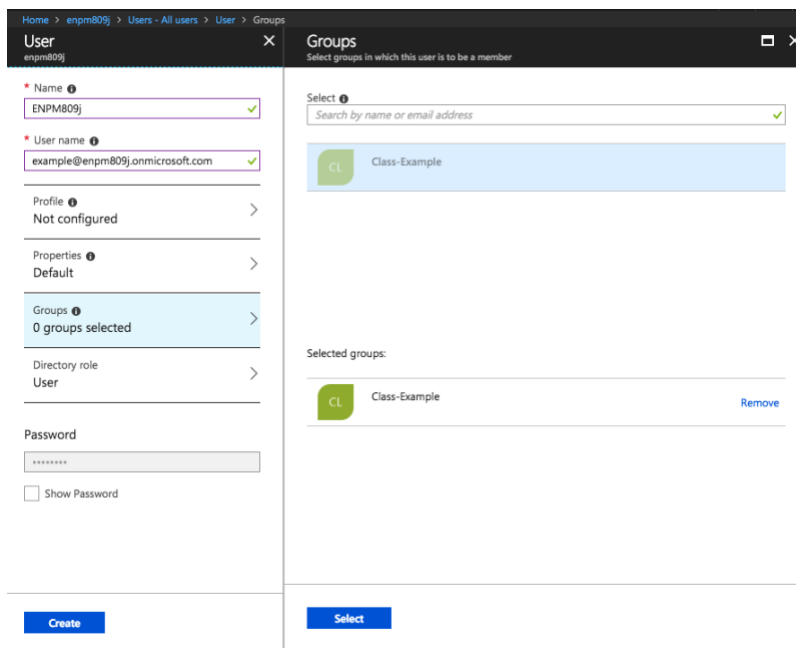
1. In the Azure portal, in the left-hand menu click the “**Azure Active Directory**” icon.



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**”

A screenshot of the 'New user' form in the Azure portal. The form is divided into two main sections: 'User' and 'Groups'. The 'User' section on the left contains fields for Name (ENPM809j), User name (example@enpm809j.onmicrosoft.com), Profile (Not configured), Properties (Default), Groups (0 groups selected), Directory role (User), and Password (masked). The 'Groups' section on the right has a search bar and a list of groups. The 'Class-Example' group is selected and appears in the 'Selected groups' list. At the bottom of the 'User' section is a 'Create' button, and at the bottom of the 'Groups' section is a 'Select' button.

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)



Sign in

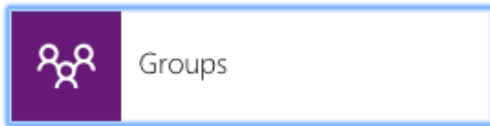
example@enpm809j.onmicrosoft.com

[Can't access your account?](#)

No account? [Create one!](#)

Next

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.



ENPM809J
ENPM809J



Groups

Search groups

Groups I own
+ Create group

No groups found

Groups I'm in
+ Join group

CL Class-Example