[version_1.1]

Note

The exercises in this course will have an associated charge in your AWS account. In this exercise, you create the following resources:

- AWS Identity and Access Management (IAM) policy, user, and role (policies, users, and roles are AWS account features, offered at no additional charge)

Familiarize yourself with the **AWS Free Tier**.

Exercise 2: Working with IAM

In this scenario, you continue to set up your new AWS account by following some security best practices with IAM.

In this exercise, you log in to your AWS account, delete the AWS account root user access keys, and (optionally) set up multi-factor authentication (MFA). You then create an IAM user with administrator access (called *Admin*). Finally, you log in as the *Admin* user and create an IAM role.

Task 1: Logging in to the AWS Management Console

In this task, you will first log in to the console as the AWS account root user.

1. Visit **https://aws.amazon.com/console/**

2. Choose **Sign In to the Console**.

3. Choose **Root user** and for **Root user email address**, enter the email address you used to create the account.

4. Choose **Next**.

5. For **Password**, enter the password for the root user.

6. Choose **Sign in**.

Task 2: Enabling MFA (optional)

In this optional task, you will enable MFA on your account by using a virtual authentication app on your mobile device or on your computer.

1. At the top right, choose your **account name**, then choose **Security credentials**.

2. Expand **Multi-factor authentication (MFA)** and choose **Activate MFA**.

3. In the **Manage MFA device** window, choose **Virtual MFA device** and then choose **Continue**.

   Note: To configure MFA for this exercise, you need to have a virtual MFA application installed on your device or computer. To see a list of MFA applications, in Step 1 of the **Set up virtual MFA device** window, choose **list of compatible applications** and scroll to **Virtual MFA Applications**. Before you continue to the next step, make sure you have installed one of the listed applications on your mobile device or on your computer.

4. Choose **Show QR code** and scan the code with your device.

   Note: If you are using a computer, choose **Show secret key**. In your MFA application, enter the secret key.

5. In the **MFA code 1** box, enter the first MFA code.

6. In the **MFA code 2** box, enter the second generated number.

7. Choose **Assign MFA**.

   You should see a window with a message that you have successfully assigned a virtual MFA device.

8. To close the window, choose **Close**.

9. Expand **Access keys (access key ID and secret access key)** and confirm that no access keys are listed.

   Note: Your account shouldn't have any listed access keys. If an access key exists (for your new account), delete the key:
   - Locate the **Actions** column and choose **Delete**.
   - In the **Delete** window, choose **Deactivate**.
   - In the confirmation box, enter the access key ID.
   - Choose **Delete**.

Task 3: Creating an IAM user

In this task, you will create an IAM user with administrator access.

1. In the **Services** search box, enter `IAM`, and open the **IAM** console.

2. In the navigation pane, choose **Users**.

3. Choose **Add users** and in the **Set user details** page, configure the following settings.
   - **User name**: `Admin`
   - **Select AWS credential type**:
     - *Access key - Programmatic access*
     - *Password - AWS Management Console access*
   - **Console password**: *Custom password* and enter a password of your choosing
   - **Require password reset**: Clear this option

4. Choose **Next: Permissions**.

5. In the **Set permission** page, choose **Attach existing policies directly**.
6. In the **Filter policies** box, search for `administrator`.
7. Under **Policy name**, select **AdministratorAccess**.
8. Choose **Next: Tags**, and then choose **Next: Review**.
9. Choose **Create user**.
10. You can sign in with the new IAM admin user by choosing the URL at the bottom of the **Success** window.

    Note: The sign-in URL should look like the following: https://123456789012.signin.aws.amazon.com/console.

11. Log in to the console with the **Admin** user and password that you created.

Task 4: Setting up an IAM role for an EC2 instance

In this task, you will log in as the *Admin* user and create an IAM role. The role allows Amazon Elastic Compute Cloud (Amazon EC2) to access both Amazon Simple Storage Service (Amazon S3) and Amazon DynamoDB. You will later assign this role to an EC2 instance that hosts the employee directory application.

1. Now that you are logged in as the *Admin* user, use the **Services** search bar to search for **IAM** again, and open the service by choosing **IAM**.
2. In the navigation pane, choose **Roles**.
3. Choose **Create role**.
4. In the **Select trusted entity** page, configure the following settings.
    - **Trusted entity type**: *AWS service*
    - **Use case**: *EC2*
5. Choose **Next**.
6. In the permissions filter box, search for `amazons3full`, and select **AmazonS3FullAccess**.
7. In the filter box, search for `amazondynamodb`, and select **AmazonDynamoDBFullAccess**.
8. Choose **Next**.
9. For **Role name**, paste `S3DynamoDBFullAccessRole` and choose **Create role**.

Note: We don’t recommend that you use full-access policies in a production environment. In this exercise, you use these policies as a proof of concept to get your exercise environment up and running quickly. After you create your S3 bucket and DynamoDB table, you can modify this IAM role so that it has more specific and restrictive permissions. You will learn more about this topic later.