[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. En el cuadro **de código MFA 2** , ingrese el segundo número generado.

7. Elija **Asignar MFA** .

   Debería ver una ventana con un mensaje que indica que ha asignado correctamente un dispositivo MFA virtual.

8. Para cerrar la ventana, elija **Cerrar** .

9. Expanda **Claves de acceso (ID de clave de acceso y clave de acceso secreta)** y confirme que no se enumeran claves de acceso.

   Nota: Su cuenta no debe tener ninguna clave de acceso en la lista. Si existe una clave de acceso (para su nueva cuenta), elimine la clave:
   - Busque la columna **Acciones** y elija **Eliminar** .
   - En la ventana **Eliminar** , seleccione **Desactivar** .
   - En el cuadro de confirmación, ingrese el ID de la clave de acceso.
   - Elija **Eliminar** .

Tarea 3: Creación de un usuario de IAM

En esta tarea, creará un usuario de IAM con acceso de administrador.

1. En el cuadro de búsqueda **Servicios** `IAM` , ingrese y abra la consola **de IAM** .

2. En el panel de navegación, elija **Usuarios** .

3. Elija **Agregar usuarios** y en la página **Establecer detalles de usuario** , configure los siguientes ajustes.
   - **Nombre de usuario** : `Admin`
   - **Seleccione el tipo de credencial de AWS** :
     - *Clave de acceso - Acceso programático*
     - *Contraseña: acceso a la Consola de administración de AWS*
   - **Contraseña de la consola** : *Contraseña personalizada* e ingrese una contraseña de su elección
   - **Requerir restablecimiento de contraseña** : borre esta opción

4. Elija **Siguiente: Permisos** .

5. En la página **Establecer permiso** , elija **Adjuntar políticas existentes directamente** .

6. En el cuadro **Políticas de filtro** , busque `administrator` .

7. En **Nombre de política** , seleccione **Acceso de administrador** .

8. Elija **Siguiente: Etiquetas** y, a continuación, elija **Siguiente: Revisar** .

9. Elija **Crear usuario** .

10. Puede iniciar sesión con el nuevo usuario administrador de IAM eligiendo la URL en la parte inferior de la ventana **Correcto** .

    Nota: La URL de inicio de sesión debe tener el siguiente aspecto: https://123456789012.signin.aws.amazon.com/console.

11. Inicie sesión en la consola con el usuario y la contraseña **de administrador** que creó.

Tarea 4: Configuración de un rol de IAM para una instancia EC2

En esta tarea, iniciará sesión como usuario *administrador* y creará un rol de IAM. El rol permite que Amazon Elastic Compute Cloud (Amazon EC2) acceda tanto a Amazon Simple Storage Service (Amazon S3) como a Amazon DynamoDB. Posteriormente, asignará este rol a una instancia EC2 que aloja la aplicación de directorio de empleados.

1. Ahora que inició sesión como usuario *administrador* , use la barra de búsqueda de **Servicios** para buscar **IAM** nuevamente y abra el servicio eligiendo **IAM** .

2. En el panel de navegación, elija **Roles** .

3. Elija **Crear rol** .

4. En la página **Seleccionar entidad de confianza** , configure los siguientes ajustes.
    - **Tipo de entidad de confianza** : *servicio de AWS*
    - **Caso de uso** : *EC2*

5. Elija **Siguiente** .

6. En el cuadro de filtro de permisos, busque `amazons3full` y seleccione **AmazonS3FullAccess** .

7. En el cuadro de filtro, busque `amazondynamodb` y seleccione **AmazonDynamoDBFullAccess** .

8. Elija **Siguiente** .

9. Para **Nombre de función** , pegue `S3DynamoDBFullAccessRole` y elija **Crear función** .

Nota : no recomendamos que utilice políticas de acceso completo en un entorno de producción. En este ejercicio, utilizará estas políticas como prueba de concepto para poner en funcionamiento rápidamente su entorno de ejercicio. Después de crear su depósito de S3 y la tabla de DynamoDB, puede modificar este rol de IAM para que tenga permisos más específicos y restrictivos. Aprenderás más sobre este tema más adelante.