

[version_1.0]

©2021 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.

Errors or corrections? Contact us at <https://support.aws.amazon.com/#/contacts/aws-training>

Exercise: Following IAM Best Practices

*The exercises are designed to be completed in your AWS account, and **will have an associated cost**. For this reason, in addition to the written instructions, this course includes video recordings of the exercises. If you intend to attempt the exercises, familiarize yourself with [AWS pricing](#), specifically [Amazon EC2 pricing](#), [Amazon S3 pricing](#), and [Amazon DynamoDB pricing](#) and the [AWS Free Tier](#).*

In this scenario, you will follow best practices while continuing to set up your new AWS account. In this exercise, you will log into the root account, delete the root user access keys, and set up multi-factor authentication (MFA).

Instead of using the root user, you will create an IAM admin user. Then, you will log in as the IAM admin user and create an IAM role that you will later assign to an EC2 instance hosting the employee directory application.

Lab Steps

Stage 1 - Login to the Console

1. Visit <https://aws.amazon.com/console/>
2. Choose **Sign In to the Console**.
3. Choose **Root user**. Enter the **Root user email address**.
4. Choose **Next**.
5. Enter the **Password** for the root user. Choose **Sign in**.

Stage 2 - Enable MFA (optional)

1. At the top right, choose your **account name**. Then choose **My Security Credentials** from the drop down menu.
2. Expand **Multi-factor authentication (MFA)**. Choose **Activate MFA**.
3. On the **Manage MFA device** pop-up window. Choose **Virtual MFA device** and choose **Continue**.

Note: You will need a virtual MFA application installed on your device or computer. You can see a list of applications on step 1 on the **Set up virtual MFA device** pop-up window. There is a hyperlink which shows a [list of compatible applications](#). Before continuing to the next step make sure you have one of these applications installed on your mobile device or computer.

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

Note: If you are using a computer you can choose **Show secret key** and type the secret key into your MFA application.

- Note:** There should be no access keys listed. If an access key exists (for your new account) choose **Delete** under **Actions**. Choose **Deactivate**. Enter in the access key ID in the confirmation field. Choose **Delete**.

1. In the service search bar, type in **Identity and Access Management (IAM)** dashboard. On the left side panel, choose **Users**.
2. Choose **Add user**. Paste in `Admin` for the **User name**. Next to **Access type**, choose **Programmatic access** and **AWS Management Console access**.
3. Next to **Console password**, choose **Custom password** and type in a password of your choosing.
4. Uncheck **Require password reset**.
5. Choose **Next: Permissions**.
6. Choose **Attach existing policies directly**. Next to **Filter policies**, search for `administrator`. Under **Policy name**, choose **AdministratorAccess**. Choose **Next: Tags**.
7. Choose **Next: Review**. Choose **Create user**.
8. You can sign in with the new IAM user by clicking the hyperlink at the bottom of the **Success** window.

Note: It should look similar to the following: <https://000000000000.signin.aws.amazon.com/console>. Your account number will be different :)
9. Log in using the **Admin** user and password that you created.

1. Now that you are logged in as the Admin user, search for **IAM** again in the service search bar. On the left side panel, choose **Roles**. Then, choose **Create role**.
2. Choose **AWS service**. Choose **EC2**. Choose **Next: Permissions**.
3. Next to **Filter policies**, search for `amazons3full` and choose **AmazonS3FullAccess**.
4. Next to **Filter policies** search for `amazondynamodb` and choose **AmazonDynamoDBFullAccess**.
5. Choose **Next: Tags**. Choose **Next: Review**.
6. For **Role name** paste in `S3DynamoDBFullAccessRole`. Choose **Create role**.

Lab Complete

2/3

For feedback, suggestions, or corrections, please contact us at: <https://support.aws.amazon.com/#/contacts/aws-training>