AWS Identity and Access Management (IAM)

EXERCISE - 5.1

Create an IAM Group

In this exercise, you will create a group for all IAM administrator users and assign the proper permissions to the new group. This will allow you to avoid assigning policies directly to a user later in these exercises.

1. Log in as the root user.
2. Create an IAM group called Administrators.
3. Attach the managed policy, IAMFullAccess, to the Administrators group.

EXERCISE - 5.2

Create a Customized Sign-In Link and Password Policy

In this exercise, you will set up your account with some basic IAM safeguards. The password policy is a recommended security practice, and the sign-in link makes it easier for your users to log in to the AWS Management Console.

1. Customize a sign-in link, and write down the new link name in full.
2. Create a password policy for your account.

EXERCISE - 5.3

Create an IAM User

In this exercise, you will create an IAM user who can perform all administrative IAM functions. Then you will log in as that user so that you no longer need to use the root user login. Using the root user login only when explicitly required is a recommended security practice (along with adding MFA to your root user).

1. While logged in as the root user, create a new IAM user called `Administrator`.
2. Add your new user to the `Administrators` group.
3. On the Details page for the administrator user, create a password.
4. Log out as the root user.
5. Use the customized sign-in link to sign in as `Administrator`.

EXERCISE - 5.4

Create and Use an IAM Role

In this exercise, you will create an IAM role, associate it with a new instance, and verify that applications running on the instance assume the permissions of the role. IAM roles allow you to avoid storing access keys on your Amazon EC2 instances.

1. While signed in as administrator, create an Amazon EC2-type role named `S3Client`.
2. Attach the managed policy, `AmazonS3ReadOnlyAccess`, to `S3Client`.
3. Launch an Amazon Linux EC2 instance with the new role attached (Amazon Linux AMIs come with CLI installed).
4. SSH into the new instance, and use the CLI to list the contents of an Amazon S3 bucket.

EXERCISE - 5.5

Rotate Keys

In this exercise, you will go through the process of rotating access keys, a recommended security practice.

1. Select the administrator, and create a two-part access key.
2. Download the access key.
3. Download and install the CLI to your desktop.
4. Configure the CLI to use the access key with the AWS Configure command.
5. Use the CLI to list the contents of an Amazon S3 bucket.
6. Return to the console, and create a new access key for the administrator account.
7. Download the access key, and reconfigure the CLI to use the new access key.
8. In the console, make the original access key inactive.
9. Confirm that you are using the new access key by once again listing the contents of the Amazon S3 bucket.
10. Delete the original access key.

EXERCISE - 5.6

Set Up MFA

In this exercise, you will add MFA to your IAM administrator. You will use a virtual MFA application for your phone. MFA is a security recommendation on powerful accounts such as IAM administrators.

1. Download the AWS Virtual MFA app to your phone.
2. Select the administrator user, and manage the MFA device.
3. Go through the steps to activate a Virtual MFA device.

4. Log off as administrator.
5. Log in as administrator, and enter the MFA value to complete the authentication process.

EXERCISE - 5.7

Resolve Conflicting Permissions

In this exercise, you will add a policy to your IAM administrator user with a conflicting permission. You will then attempt actions that verify how IAM resolves conflicting permissions.

1. Use the policy generator to create a new policy.
2. Create the policy with Effect: Deny; AWS Service: Amazon S3; Actions: *; and ARN: *.
3. Attach the new policy to the `Administrators` group.
4. Use the CLI to attempt to list the contents of an Amazon S3 bucket. The policy that allows access and the policy that denies access should resolve to deny access.