This lab demonstrates the steps from *Demo: Assign IAM Permissions and Group and Users.*
My full AWS Architect Associate course can be found here:
https://www.udemy.com/course/ultimateaws/?referralCode=7ED214B795C444141361

Lab Guide: IAM Users, Groups, and Policies in AWS

Objective:

- Understand IAM users, groups, and policies.
- Learn how to create and manage users, attach policies, and utilize groups for efficient permission management.

---

1. Accessing the IAM Dashboard

Steps:

1. **Log in to the AWS Console.**
   - Navigate to the **IAM Dashboard** by searching for "IAM" in the AWS Console search bar.
2. **Observe Global Scope:**
   - Note that the region automatically changes to **Global** when accessing IAM.
   - IAM configurations apply across all AWS regions.

Key Concept:

- **IAM Global Service:** IAM settings are global and not tied to specific regions.

---

2. Understanding IAM Users

Definition:

- **IAM User**: A digital identity in AWS associated with one individual in real life. Each user has a unique set of credentials for accessing AWS resources.

Steps to Create a User:

1. In the IAM Dashboard, click **"Users"** in the left-hand menu, then click **"Create user."**
2. Enter a username (e.g., "Rick").
3. Choose **"AWS Management Console Access"** to allow the user to log in to the console.
4. Create a password:
    - Optionally, enable **"Require Password Reset"** for first-time login.
5. **Access Keys**:
    - Do **not** create access keys unless the user requires programmatic access via the AWS CLI, SDK, or API.
    - Access keys should only be generated when necessary for enhanced security.
6. Click **"Next"** to proceed to permissions.

Key Concepts:

- **Console Access**: Grants the user the ability to log in via the AWS Management Console.
- **Access Keys**: Credentials for programmatic access; use them sparingly to reduce security risks.

---

3. Attaching Policies to Users

Definition:

- **Policy**: A document defining permissions (e.g., access to specific services and actions). Policies control what a user can and cannot do in AWS.

Steps to Attach a Policy:

1. Choose **"Attach existing policies directly"** for the user.
2. Search for a policy (e.g., type "S3").
    - Example: **"AmazonS3FullAccess"** allows full access to S3.
    - Alternatively, select **"AmazonS3ReadOnlyAccess"** for read-only permissions.
3. Select the desired policy and attach it to the user.

Key Concepts:

- **AWS Managed Policies**: Predefined policies created and maintained by AWS.
- **Customer Managed Policies**: Custom policies created by you to meet specific needs.

---

4. Using IAM Groups for Efficient Permission Management

Definition:

- **IAM Group**: A collection of users sharing the same permissions. Permissions are assigned to the group, and all users in the group inherit them.

Steps to Create a Group:

1. In the IAM Dashboard, click **"User groups"** in the left-hand menu, then click **"Create group."**
2. Enter a group name (e.g., "Admins").
3. Assign permissions to the group:
    - Search for the policy **"AdministratorAccess."**
    - Select this policy to grant full administrative privileges to the group.
4. Click **"Create user group."**

Adding Users to the Group:

1. Go to the **"Users"** section and select the user you want to add (e.g., "Rick").
2. Click **"Add to Groups."**
3. Select the appropriate group (e.g., "Admins") and confirm.

Key Concept:

- **Group Benefits**: Managing permissions at the group level simplifies administration and reduces the risk of inconsistencies when dealing with multiple users.

---

5. Exploring Policies in Detail

Types of Policies:

1. **AWS Managed Policies**:
    - Maintained by AWS and regularly updated to follow best practices.
    - Example: **"AmazonS3FullAccess"**.
2. **Customer Managed Policies**:
    - Created and customized by the account owner for specific use cases.
    - Example: A policy restricting access to specific S3 buckets.

Steps to Create a Custom Policy:

1. In the IAM Dashboard, click **"Policies"** and select **"Create Policy."**
2. Use the **Visual Editor** or write the policy in JSON format.
3. Define actions, resources, and conditions for the policy.
4. Save the policy and attach it to a user, group, or role as needed.

Key Concept:

- **Policy Attachment**: Policies can be attached directly to users or indirectly via groups. Group-level management is preferred for better scalability.

---

6. Best Practices for IAM

1. **Use Groups**:
    - Always assign permissions at the group level when possible.

    - Avoid attaching policies directly to individual users.
2. **Enable MFA**:
    - Require multi-factor authentication for all users, especially those with elevated privileges.
3. **Follow the Principle of Least Privilege**:
    - Grant only the permissions a user or group needs to perform their job.
4. **Avoid Using Root Account for Daily Tasks**:
    - Reserve the root account for account and billing management.
5. **Regularly Review IAM Policies**:
    - Audit permissions to ensure they align with current business needs.

Summary:

In this lab, you:

- Learned about IAM users, groups, and policies.
- Created an IAM user and assigned permissions directly via policies.
- Created an IAM group, assigned permissions to the group, and added users to it.
- Explored AWS-managed and customer-managed policies.

By following these steps, you can effectively manage access and permissions in AWS, ensuring a secure and scalable environment.