Step-by-Step Guide to Create an IAM User, IAM Policy, and IAM Group in AWS

Prerequisites

1. An AWS account with administrative privileges.
2. Basic understanding of AWS Identity and Access Management (IAM).

Step 1: Create an IAM Group

1. **Log in to the AWS Management Console**:

    - Go to the AWS Management Console.
    - Sign in with your credentials.

2. **Navigate to the IAM Dashboard**:

    - In the AWS Management Console, search for **IAM** in the search bar.
    - Click on **IAM** to open the IAM dashboard.

3. **Create a New IAM Group**:

    - In the left-hand menu, click on **User Groups**.
    - Click the **Create group** button.
    - Enter a **Group name** (e.g., `Developers`).
    - (Optional) Attach policies to the group at this stage (you can skip this and attach policies later).
    - Click **Create group**.

Step 2: Create an IAM Policy

1. **Navigate to the Policies Section**:

    - In the IAM dashboard, click on **Policies** in the left-hand menu.
    - Click the **Create policy** button.

2. **Configure the Policy**:

   - Go to the **JSON** tab and paste the following complex policy:

     ```
     {
       "Version": "2012-10-17",
       "Statement": [
         {
           "Effect": "Allow",
           "Action": [
             "ec2:StartInstances",
             "ec2:StopInstances"
           ],
           "Resource": "*"
         },
         {
           "Effect": "Deny",
           "Action": [
             "ec2:StopInstances",
             "ec2:TerminateInstances"
           ],
           "Resource": "arn:aws:ec2:region:account-id:instance/instan
         }
       ]
     }
     ```

     Replace the following placeholders:

     - `region` : The AWS region where the EC2 instance is located (e.g., `us-east-1`).
     - `account-id` : Your AWS account ID.
     - `instance-id` : The ID of the specific EC2 instance you want to restrict (e.g., `i-0123456789abcdef0`).

3. **Review and Create the Policy**:

   - Provide a **Policy name** (e.g., `EC2-StartStop-DenySpecificInstance`).
   - (Optional) Add a description for the policy.
   - Click **Create policy**.

Step 3: Attach the Policy to the IAM Group

1. **Navigate to the IAM Group**:

- Go back to the **User Groups** section in the IAM dashboard.
- Select the group you created earlier (e.g., `Developers`).

2. **Attach the Policy**:

    - Click on the **Permissions** tab.
    - Click **Add permissions** and select **Attach policies**.
    - Search for the policy you created (e.g., `EC2-StartStop-DenySpecificInstance`).
    - Select the policy and click **Add permissions**.

Step 4: Create an IAM User

1. **Navigate to the Users Section**:

    - In the IAM dashboard, click on **Users** in the left-hand menu.
    - Click the **Add users** button.

2. **Configure the User**:

    - Enter a **User name** (e.g., `JohnDoe`).
    - Select **Provide user access to the AWS Management Console**.
    - Choose **I want to create an IAM user**.
    - Set a custom password or let AWS generate one.
    - (Optional) Require the user to reset their password on first login.
    - Click **Next**.

3. **Add the User to the Group**:

    - On the **Set permissions** page, select **Add user to group**.
    - Choose the group you created earlier (e.g., `Developers`).
    - Click **Next**.

4. **Review and Create the User**:

    - Review the user details and permissions.
    - Click **Create user**.

5. **Download User Credentials**:

    - After the user is created, download the `.csv` file containing the user's sign-in URL, username, and password.

Step 5: Test the IAM User

1. **Log in as the IAM User**:
    - Use the sign-in URL provided in the `.csv` file.
    - Enter the username and password for the IAM user.
2. **Verify Permissions**:
    - Try starting and stopping EC2 instances. This should work for all instances except the specific one mentioned in the policy.
    - Attempt to stop or terminate the specific EC2 instance. This should be denied.

Step 6: Clean Up (Optional)

1. **Delete the IAM User**:
    - Go to the **Users** section in the IAM dashboard.
    - Select the user and click **Delete user**.
2. **Delete the IAM Group**:
    - Go to the **User Groups** section.
    - Select the group and click **Delete group**.
3. **Delete the IAM Policy**:
    - Go to the **Policies** section.
    - Select the policy and click **Delete policy**.

Conclusion

You have successfully created an IAM user, IAM policy, and IAM group in AWS. The policy allows starting and stopping all EC2 instances but denies stopping and terminating a specific EC2 instance. This demonstrates how to use both **Allow** and **Deny** statements in IAM policies for fine-grained access control.