User and Group Management Documentation

Overview

AWS Identity and Access Management (IAM) is a powerful service that enables secure control of access to AWS resources. This document outlines a step-by-step process for managing IAM users and groups to ensure secure and efficient resource management.

Step-by-Step Guide

1. Creating an IAM User

Objective: Create a new IAM user with restricted access to specific AWS services.

- **Action:**
  1. Log in to the AWS Management Console as the root user.
  2. Navigate to the IAM service.
  3. Select **Users** from the left-hand menu and click **Add users**.
  4. Enter a username (e.g., `s3-user`).
  5. Choose the **Access type**:
     - **AWS Management Console access** for password-based login.
     - **Programmatic access** for API and CLI interactions (generates an access key).
  6. Assign the user an existing policy or create a custom policy granting **S3 access only**.
  7. Review and create the user.
- **Result:** The user is created with restricted access to only the S3 service.

2. Generating Login Credentials

Objective: Provide the IAM user with secure login credentials.

- **Action:**
  1. During user creation, generate credentials:
     - **Console login password:** Can be set manually or autogenerated.
     - **Access key ID and secret access key:** Required for API/CLI usage.
  2. Download the credentials file or copy the details securely.
- **Result:** The IAM user receives secure credentials to access allowed services.

3. Testing Restricted Access

Objective: Ensure the IAM user has access only to assigned resources.

- **Action:**
  1. Log in using the IAM user credentials.
  2. Attempt to access the S3 service (allowed).
  3. Attempt to access other services like EC2 (denied).
- **Result:** Access control policies are validated, ensuring the user can access only S3 while being restricted from other services.

4. Setting Up a Group

Objective: Manage permissions for multiple users efficiently by creating an IAM group.

- **Action:**
  1. Navigate to the **Groups** section in the IAM Console.
  2. Click **Create New Group** and name it (e.g., `group-01`).
  3. Add users to the group:
     - Select users from the available list (e.g., `s3-user` and `ec2-user`).
- **Result:** The group is created and associated with the selected users.

5. Assigning Group Permissions

Objective: Grant permissions to a group to manage access at scale.

- **Action:**
  1. Attach policies to the group by selecting the **Permissions** tab.
  2. Assign existing policies (e.g., `AmazonS3FullAccess` and `AmazonEC2FullAccess`).
  3. Specify that any additional service permissions must be explicitly requested from the root user.
- **Result:** Group members inherit permissions to S3 and EC2 services while maintaining restricted access to other resources.

Key Learnings

- **Granular Control:** IAM allows precise control of user and group access, ensuring cloud security.
- **Scalability:** Group management simplifies permission handling for multiple users.
- **Best Practices:** Always use the principle of least privilege and avoid using root user credentials for daily operations.

Conclusion

This exercise demonstrated the power of AWS IAM in securing cloud resources and managing user access effectively. By following these steps, organizations can ensure a secure and scalable access control strategy for their AWS environment.