Author: Madhurima Rawat

Cloud Security: Identity and Access Management (IAM)

This experiment focuses on managing users, permissions, and security policies in the cloud using AWS Identity and Access Management (IAM). It provides hands-on experience in configuring access controls, defining security policies, and ensuring proper authorization within cloud environments. The setup utilizes Docker, LocalStack, and AWS CLI to simulate IAM functionalities, enabling the creation and management of users, roles, and policies in a local cloud-like environment.

This document provides a comprehensive breakdown of all commands, inputs, outputs, and their explanations, ensuring a clear understanding of each step in the workflow.

1. Creating an IAM User

Command:

```
aws iam create-user --user-name test-user
--endpoint-url=%AWS_ENDPOINT_URL%
```

Explanation:

- `aws iam create-user` → Creates a new IAM user.
- `--user-name test-user` → Specifies the user name as `test-user`.
- `--endpoint-url=%AWS_ENDPOINT_URL%` → Uses a custom endpoint.

Output:

```
---

## | IAM User Info |

| Arn         | arn:aws:iam::000000000000:user/test-user |
| CreateDate  | 2025-03-06T15:43:02.050000Z |
| Path        | / |
| UserId      | 7ll7td3a2x1shy4p7x2b |
| UserName    | test-user |

---
```

Output Breakdown:

- `Arn` : Unique identifier for the user.
- `CreateDate` : Timestamp when the user was created.
- `Path` : Default path, `/` .
- `UserId` : System-generated unique identifier.
- `UserName` : The specified user name.

2. Creating an IAM Role

Command:

```
aws iam create-role --role-name ec2-role
--assume-role-policy-document file://trust-policy.json
--endpoint-url=%AWS_ENDPOINT_URL%
```

Explanation:

- `aws iam create-role` → Creates a new IAM role.
- `--role-name ec2-role` → Specifies the role name as `ec2-role` .
- `--assume-role-policy-document file://trust-policy.json` → Specifies the trust policy file.
- `--endpoint-url=%AWS_ENDPOINT_URL%` → Uses a custom endpoint.

Output:

```
---

## | IAM Role Info |

| Arn          | arn:aws:iam::000000000000:role/ec2-role |
| CreateDate   | 2025-03-06T15:44:48.493000Z |
| Path         | / |
| RoleId       | AROAQAAAAAAANMF4UL4W3 |
| RoleName     | ec2-role |

## | AssumeRolePolicyDocument |

| Version    | 2012-10-17 |
| Action     | sts:AssumeRole |
| Effect     | Allow |
| Principal  | Service: ec2.amazonaws.com |

---
```

Output Breakdown:

- `Arn` : Unique identifier for the role.
- `CreateDate` : Timestamp of role creation.
- `Path` : Default path, `/` .
- `RoleId` : System-generated unique identifier.
- `RoleName` : The specified role name.
- `AssumeRolePolicyDocument` : Defines who can assume the role.

3. Attaching a Policy to the IAM User

Command:

```
aws iam attach-user-policy --user-name test-user --policy-arn
arn:aws:iam::aws:policy/AdministratorAccess
--endpoint-url=%AWS_ENDPOINT_URL%
```

Explanation:

- `aws iam attach-user-policy` → Attaches a policy to a user.
- `--user-name test-user` → Specifies the user `test-user` .
- `--policy-arn arn:aws:iam::aws:policy/AdministratorAccess` → Grants Administrator Access.
- `--endpoint-url=%AWS_ENDPOINT_URL%` → Uses a custom endpoint.

Output:

No explicit output for this command.

Output Breakdown:

- No direct output, but the user gets assigned the specified policy.

4. Listing IAM Users

Command:

```
aws iam list-users --endpoint-url=%AWS_ENDPOINT_URL%
```

Output:

```
---

## | IAM Users |

| Arn          | arn:aws:iam::000000000000:user/test-user |
| CreateDate   | 2025-03-06T15:43:02.050000Z |
| Path         | / |
| UserId       | 7ll7td3a2x1shy4p7x2b |
| UserName     | test-user |

---
```

Output Breakdown:

- Lists all IAM users with their details.

5. Listing IAM Roles

Command:

```
aws iam list-roles --endpoint-url=%AWS_ENDPOINT_URL%
```

Output:

```
---

## | IAM Roles |

| Arn                 | arn:aws:iam::000000000000:role/ec2-role |
| CreateDate          | 2025-03-06T15:44:48.493575Z |
| MaxSessionDuration | 3600 |
| Path                | / |
| RoleId              | AROAQAAAAAAANMF4UL4W3 |
| RoleName            | ec2-role |

## | AssumeRolePolicyDocument |

| Version    | 2012-10-17 |
| Action     | sts:AssumeRole |
| Effect     | Allow |
| Principal  | Service: ec2.amazonaws.com |
---
```

Output Breakdown:

- Lists all IAM roles with their attributes.
- Includes assume role policy details.

6. Listing Attached Policies for the IAM User

Command:

```
aws iam list-attached-user-policies --user-name
test-user --endpoint-url=%AWS_ENDPOINT_URL%
```

Output:

```
---

## | Attached Policies |

| PolicyArn                                    | PolicyName |
|--------------------------------------------|------------------|
| arn:aws:iam::aws:policy/AdministratorAccess | AdministratorAccess |

---
```

Output Breakdown:

- Displays policies attached to the specified IAM user.
- Shows the policy ARN and name.