[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+alnafi07+2025_02+type@vertical+block@bee6449553c64c94a4db4dffbfb44e74?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Lab 7: AWS Identity and Access Management (IAM)**

*RQF Level 5*

**Objective:**

The objective of this lab is to provide participants with hands-on experience in AWS Identity and Access Management (IAM). Participants will learn to create and manage IAM users, groups, and roles, explore policy definitions, and implement access controls to enhance security and user management in their AWS environment.

**Prerequisites:**

* SysOps Advancement Track

**Lab Steps:**

**Step 1: Introduction to AWS IAM**

- Briefly discuss the importance of IAM in AWS security.

- Introduce key IAM concepts, including users, groups, roles, and policies.

**Step 2: Creating IAM Users**

- In the AWS Management Console, navigate to IAM.

- Create IAM users with programmatic access.

- Configure password policies and multi-factor authentication (MFA) for users.

**Step 3: Creating IAM Groups**

- Create IAM groups and add users to groups.

- Assign policies to groups to manage permissions efficiently.

- Discuss the advantages of using groups for access control.

**Step 4: Creating IAM Roles**

- Create IAM roles with specific permissions.

- Discuss scenarios where roles are beneficial, such as cross-account access and temporary permissions.

- Understand the concept of trust policies associated with roles.

**Step 5: Defining IAM Policies**

- Explore IAM policies and understand JSON policy language.

- Create custom IAM policies for fine-grained access control.

- Attach policies to users, groups, and roles.

**Step 6: Testing IAM Access**

- Simulate different access scenarios:

- Test IAM user access to specific AWS services.

- Evaluate group-based permissions.

- Assume IAM roles and verify permissions.

**Step 7: IAM Access Analyzer**

- Explore IAM Access Analyzer to identify and manage resource access risks.

- Review generated findings and take corrective actions.

**Step 8: Cleanup**

- Guide learners through proper cleanup procedures to avoid unnecessary costs.

- Delete IAM users, groups, roles, and policies created during the lab.

*Conclusion:*

*By completing this lab, participants have gained practical experience in AWS Identity and Access Management. They have learned to create and manage IAM users, groups, and roles, define IAM policies, and implement access controls to ensure secure and efficient user management in AWS. This lab provides a foundation for understanding IAM best practices and security principles in AWS environments.*