[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+alnafi07+2025_02+type@vertical+block@a25096782f214371a540c759d3b1a21d?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Lab 6: Secure Architecture Design**

*RQF Level 5*

**Objective:**

The objective of this lab is to guide participants in setting up a secure AWS environment by establishing a Virtual Private Cloud (VPC) with public and private subnets. Participants will configure Security Groups, Network Access Control Lists (NACLs), and implement best security practices to enhance the overall security posture of their AWS infrastructure.

**Prerequisites:**

* SysOps Advancement Track

**Lab Steps:**

**Step 1: Introduction to Secure Architecture Design on AWS**

- Briefly discuss the importance of security in cloud environments.

- Introduce the concept of Virtual Private Cloud (VPC) and the need for public and private subnets.

**Step 2: Creating a VPC**

- In the AWS Management Console, navigate to Amazon VPC.

- Create a new VPC with appropriate CIDR blocks.

- Configure public and private subnets across multiple availability zones.

**Step 3: Configuring Security Groups**

- Define Security Groups for instances in both public and private subnets:

- Public subnet Security Group: Allow inbound traffic for specific services (e.g., HTTP, HTTPS) and necessary outbound traffic.

- Private subnet Security Group: Allow outbound traffic and only allow inbound traffic from the public subnet.

**Step 4: Configuring Network ACLs (NACLs)**

- Create Network ACLs for the VPC:

- Define rules for inbound and outbound traffic for both public and private subnets.

- Emphasize the statelessness of NACLs and their role in controlling traffic at the subnet level.

**Step 5: Configuring Internet Gateway and Route Tables**

- Attach an Internet Gateway to the VPC.

- Configure route tables for public and private subnets:

- Public subnet route table: Route traffic to the Internet Gateway.

- Private subnet route table: Route traffic to the local network and optionally through a NAT gateway.

**Step 6: Testing Connectivity and Security**

- Launch instances in both public and private subnets.

- Verify connectivity within the VPC and to the internet.

- Test security by attempting to access resources from unauthorized locations.

**Step 7: Implementing Best Security Practices**

- Discuss and implement additional security best practices:

- Key pair management for SSH access.

- Enabling VPC Flow Logs for network traffic monitoring.

- Using AWS Identity and Access Management (IAM) for fine-grained access control.

**Step 8: Cleanup**

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

- Delete the VPC, instances, Internet Gateway, and any other resources created during the lab.

*Conclusion:*

*By completing this lab, participants have gained practical experience in designing and implementing a secure architecture on AWS. They have learned how to set up a VPC with public and private subnets, configure Security Groups and Network ACLs, and implement best security practices. This lab provides a foundation for building secure and resilient AWS environments.*