[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+alnafi07+2025_02+type@vertical+block@9a95ea8e203446548843c075d9c6499f?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Lab 10: Capstone Project - Comprehensive AWS Solution Design**

*RQF Level 5*

**Objective:**

The objective of this capstone project is to integrate the knowledge gained from previous labs and design a comprehensive, end-to-end AWS solution. Participants will design a multi-tier, scalable, and secure application infrastructure on AWS, incorporating DevOps practices, SysOps monitoring, security best practices, and Governance, Risk, and Compliance (GRC) considerations.

**Prerequisites:**

* DevOps Advancement Track
* SysOps Advancement Track

**Lab Steps:**

**Step 1: Define Application Requirements**

- Clearly define the requirements of the application, considering factors such as scalability, availability, and security.

- Identify the services and resources required to meet these requirements.

**Step 2: Architect the Multi-Tier Infrastructure**

- Design a multi-tier infrastructure that includes front-end, application, and database tiers.

- Leverage AWS services such as Amazon EC2, Amazon RDS, and Amazon S3.

- Consider the use of load balancing for distributing traffic and ensuring high availability.

**Step 3: Implement DevOps Practices**

- Set up a CI/CD pipeline using AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy.

- Integrate version control, automated testing, and automated deployment into the pipeline.

- Implement Infrastructure as Code (IaC) using tools like AWS CloudFormation or Terraform.

**Step 4: SysOps Monitoring and Management**

- Configure Amazon CloudWatch for monitoring key metrics.

- Set up alarms for proactive alerting.

- Implement logging and tracing using AWS CloudWatch Logs and AWS X-Ray.

**Step 5: Implement Security Best Practices**

- Apply security best practices for IAM, including user roles, groups, and policies.

- Leverage AWS Key Management Service (KMS) for encryption of data at rest.

- Implement network security using Security Groups and Network Access Control Lists (NACLs).

**Step 6: GRC Considerations**

- Implement resource tagging for cost allocation and management.

- Explore AWS Organizations for centralized account management and control.

- Implement and test Service Control Policies (SCPs) for governance.

**Step 7: Test and Validate the Solution**

- Deploy the designed solution in the AWS environment.

- Conduct testing to ensure scalability, availability, and security.

- Validate that the implemented DevOps practices streamline the development and deployment process.

**Step 8: Documentation**

- Create comprehensive documentation for the designed AWS solution, including architecture diagrams, security measures, and DevOps processes.

- Include details on monitoring, logging, and compliance aspects.

**Step 9: Presentation**

- Prepare a presentation to showcase the designed AWS solution.

- Highlight key features, security measures, scalability considerations, and GRC aspects.

- Be ready to discuss the reasoning behind design decisions.

**Step 10: Cleanup**

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

- Delete the AWS resources created during the capstone project.

*Conclusion:*

*This capstone project challenges participants to apply their knowledge and skills acquired from previous labs to design a comprehensive AWS solution. It emphasizes the integration of DevOps practices, SysOps monitoring, security best practices, and GRC considerations in a real-world scenario. The project provides a holistic understanding of AWS services and their practical application in building robust and secure cloud architectures.*