



Diploma in DevSysOps Engineering

EduQual Level 5 Endorsed Diploma

Learner Handbook
AL NAFI INTERNATIONAL COLLEGE
<https://alnafi.com>

Version: 1.0

Issue Date: [Insert Date]

© 2021 Al Nafi E-Learning Private Limited. All rights reserved.

Table of Contents

1. About the Diploma	4
2. Key Features of the Diploma	4
3. About the Diploma Program Endorsed by EduQual	5
4. About Al Nafi International College	5
5. Program Eligibility Criteria and Application Process	6
5.1. Eligibility Criteria	6
5.2. Application Process	6
6. Connect with the Support Operations Center	7
7. Program Outcomes	7
8. Who Should Enrol in this Program?	8
9. Learning Path	9
10. Assessment Information	10
10.1. Assessment Overview	10
Assessment Components	10
10.2. Al Razzaq Lab Assignments (70% weightage in overall Grade)	11
What Are They?	11
How Are They Graded?	11
What If You Need to Resubmit?	11
10.3. Multiple Choice Questions (15% of Your Grade)	11
Assessment Format	11
Attempts and Scoring	12
Diploma Program Access Period	12
10.4. English Language Exam (15% of Your Grade)	12
Mandatory Requirement	12
Submission Requirements	12
Verification and Compliance	13
Why Is This Required?	13
10.5. Al Razzaq Labs Program Access	13
Prerequisites for Lab Access	13
Lab Components	13
Additional Features and Support	14
10.6. Grading Criteria	14
Grade Boundaries	14
Example Calculation	
For a student:	15
Example: Overall Grade Calculation	16
Quick Reference Table	16
10.7. Academic Integrity	17
Violation Response	17
10.8. Support for Students	18
10.9. Accessibility and Reasonable Adjustments	18
10.10. Appeals Process	18

Complete Course Units	19
Unit 1: Linux Deep Dive	19
Unit 2: Python Deep Dive	19
Unit 3: Certified Information Systems Security Professional (CISSP)	20
Unit 4: Red Hat Enterprise Linux (RHEL)	20
Unit 5: AWS Solutions Architect	21
Unit 6: Python Automation	22
Unit 7: Certified Kubernetes Application Developer (CKAD)	22
Unit 8: Certified Kubernetes Administrator (CKA)	23
Unit 9: Ansible Deep Dive	24
Unit 10: DevOps Docker Deep Dive	24
Unit 11: Certificate of Cloud Security Knowledge (CCSK)	25
Unit 12: Certified Kubernetes Security Specialist (CKS)	26
Unit 13: Python Flask	26
Unit 14: Python Selenium	27
Unit 15: Docker Deep Dive I	27
Unit 16: Bash Script Deep Dive I	28
Unit 17: Python Automation Deep Dive I	29
Unit 18: Python Selenium I	30
Unit 19: JIRA with Python I	32
Unit 20: Python Flask I	33
Unit 21: Vagrant I	34
Unit 22: Ansible I	35
Unit 23:Kubernetes Application Developer I	36
Unit 24: Kubernetes and Cloud Native Associates I	37
Unit 24: Kubernetes Administrator I	39
Unit 26: Kubernetes Security Specialist I	40
Unit 27: AWS Solution Architecture I	41
Unit 28: Microsoft Azure Administrator I	42
Unit 29: Professional Cloud Security I	43
Unit 30: Cloud Security Standards Review I	44
Unit 31: ISSAP Architecture Professional Review I	46
Unit 32: Cloud Assurance: Zero Trust Frameworks	47
Unit 33: LinkedIn Course for Job Seekers	47
Unit 34: IELTS Academic and General Training	48
COPYRIGHT NOTICE	49
Unauthorized Use Prohibited	49

1. About the Diploma

Introducing the "Diploma in DevSysOps Engineering" - Your Path to a Dynamic Tech Career

The "Diploma in DevSysOps Engineering" is an all-encompassing program, designed to equip learners with the essential skills and knowledge required for thriving careers in DevOps, SysOps, Cloud Engineering, and Cloud Cyber Security. This diploma curriculum consists of an array of meticulously crafted courses, each focused on core aspects within these dynamic fields.

Our learners will explore units that integrate DevOps, SysOps, and cybersecurity practices into a comprehensive learning experience.

One distinguishing feature of this program is the hands-on learning experience it offers. Through our home grown Al Razzaq labs, learners will access cloud computing labs and container labs. This hands-on approach is thoughtfully integrated throughout the curriculum, providing learners with a holistic understanding of system design, development, deployment, maintenance, and problem-solving.

Upon successfully completing this diploma program, our learners are well-prepared to embark on promising careers in DevOps and SysOps. Within a relatively short period, typically 3 to 6 months, our graduates often secure positions such as AWS Cloud Compliance Manager, Cloud Security Architect, DevSecOps Specialist, DevOps Engineers, Automation Engineers, Cloud Architects, and System Administrators, both within their home countries and internationally.

Moreover, this diploma program seamlessly integrates specific units from the Diploma in Cloud Cyber Security (EduQual Level 3), the Diploma in DevOps and Cloud Advancement (EduQual Level 4), and the Diploma in SysOps and Cloud Advancement (EduQual Level 4). This approach empowers learners to cultivate a more comprehensive understanding of emerging technologies, expanding their knowledge base and enhancing their employability through diversified expertise.

The program focuses on employability by providing access to open-source, vendor-neutral resources, instructional videos, practical hands-on labs, and various assessments, while also securing admission into the final year of a Bachelor's degree program. To enrich the practical learning experience, step-by-step guidance is offered, and learners can interact with instructors through community engagement, discussion forums, and live online classes.

In essence, the "Diploma in DevSysOps Engineering" at EduQual Level 5 is a comprehensive and practical program, meticulously designed to prepare learners for thriving careers in the dynamic fields of DevOps, SysOps, Cloud Engineering, and Cyber Security. Graduates of this program are poised to excel in the technology industry, benefiting from hands-on experience and a curriculum finely tuned to meet the demands of the job market, making them job-ready within 3 to 6 months.

2. Key Features of the Diploma

- EduQual endorsement, a globally recognised qualification.

- Nearly 2000 hours of hands-on cloud labs integrated across all units
- Delivered through Self-paced online and distance learning..
- Job description-led learning aligned with industry roles
- 8X higher live interaction through live online classes conducted by industry experts
- Vibrant student communities for peer support and networking
- Professional resume building and Internship programme eligibility services through AI Razzaq Program
- Undergraduate programme progression pathways
- Gain full expertise in Cloud Environments with Cloud Playground's on-demand servers and specialised containers for every lab scenario

3. About the Diploma Program Endorsed by EduQual

The Diploma in DevSysOps Engineering, endorsed by EduQual at Level 5, holds significant value for those seeking careers in Cyber Security, Cloud Computing, SysOps and DevOps. As a globally recognized awarding organisation, EduQual provides top-tier qualifications that are widely respected by employers and academic institutions worldwide. The endorsement of the Diploma in DevSysOps Engineering demonstrates the program's commitment to upholding high-quality standards and providing students with comprehensive training in cloud computing. This diploma is an excellent option for individuals looking to improve their SysOps and DevOps methodologies and cloud computing abilities while enhancing their career opportunities in this rapidly changing sector. Moreover, since the diploma is equivalent to Level 5 of the Regulated Qualifications Framework (RQF), learners who acquire the EduQual certificate may be eligible for a second-year exemption in an undergraduate degree program.

Upon completion of this diploma program, students will:

- Receive one Certificate and one transcript of EduQual diploma after completion of the program.
- Eligible for AI Nafi Alumni membership and admission in third year Bachelor's Degree programs.
- Apply for jobs based upon the skills of the student who does not want to take admission.

4. About AI Nafi International College

AI Nafi International College, the leading global e-Learning platform, offers rigorous and specialized training in emerging technologies and processes shaping the digital landscape. With a cost-effective, self-paced learning and time-efficient approach, we have served more than 300,000 learners, with numerous alumni excelling in Fortune 500 companies worldwide. Our diploma programs are designed to help both students, professionals and organizations achieve their career and business objectives.

5. Program Eligibility Criteria and Application Process

To apply for the DevSysOps Engineering diploma at Eduqual Level 5, individuals who are interested will need to register for the diploma through the website. The provided link <https://alnafi.com/courses/diploma-in-devsysops-engineering> can be used by learners to complete their application.

To enrol in this diploma, individuals just need to have studied up to at least grade 12, or hold a Level 3 qualification – for example Intermediate, A Level, IB diploma, a Pearson BTEC Level 3, or any equivalent qualification.

A student who has any Level 4 certificate or an equivalent qualification can also take admission in this diploma.

5.1. Eligibility Criteria

To enrol in this diploma, individuals just need to have studied up to at least grade 12, or hold a Level 3 qualification – for example Intermediate, A Level, IB diploma, a Pearson BTEC Level 3, or any equivalent qualification.

A student who has any Level 4 certificate or an equivalent qualification can also take admission in this diploma.

All learners must possess the following:

- A laptop with an average specification or desktop computer that is in good working order.
- A dependable internet connection.
- Proficiency in using the internet and the ability to troubleshoot internet-related issues.

5.2. Application Process

After selecting the preferred payment plan, learners can begin their studies with ease as the application process comprises only three straightforward steps.

STEP 1

CHOOSE THE PAYMENT PLAN AND TYPE

Fill out the application form and choose your preferred payment plan, which includes options for monthly, quarterly, half-yearly, and annual payments.

STEP 2

SUBMIT THE APPLICATION PROCESS

With just one click, submit your application once you have chosen the payment method and plan.

STEP 3

COMPLETE KYS VERIFICATION

After payment, complete the KYS form and upload your previous qualification documents for verification. Course access will only be provided after the KYS verification process is completed successfully.

STEP 4

ADMISSION

Once your KYS have been completed and verified, immediately begin your studies. Access to the student portal might take 24 to 48 hours to verify. If there are issues in accessing the Al Nafi student portal then learners should connect with support through call, message on the number given on the website. Or either through email at support@alnafi.com

6. Connect with the Support Operations Center

Our dedicated support team is here to assist you with any questions or concerns you may have regarding the application process and related matters, 24/7. They can help you with inquiries regarding

- the application.
- provide information on the course and labs and assessments.
- Guide about job aspects
- Guide about admission by using this diploma.
- clarify any confusion you have about the diploma program.

7. Program Outcomes

- Analyse and implement Docker containerisation strategies, integrating seamlessly with AWS to manage scalable cloud deployments.
- Apply advanced Bash scripting to automate and optimise DevOps and SysOps workflows, ensuring efficient cloud management on AWS.
- Design and implement Python automation frameworks to streamline and enhance the efficiency of core DevOps and SysOps processes.
- Utilise Python Selenium to construct automated task solutions specifically tailored for execution within AWS DevSysOps environments.
- Construct and evaluate Python-Jira integrations to optimise operational workflows across DevOps, SysOps, Cloud Security, Cybersecurity, and GRC frameworks.
- Develop and deploy Flask-based micro web applications, applying them to solve complex challenges within AWS DevSysOps projects.
- Analyse Vagrant's role within DevSysOps and apply its capabilities to manage reproducible, portable development environments in AWS.
- Apply Ansible automation to configure, manage, and scale AWS infrastructure effectively, interpreting outcomes to refine system performance.
- Develop and manage containerised applications using Kubernetes, evaluating deployment strategies within AWS environments.
- Evaluate and implement cloud-native Kubernetes architectures on AWS to construct highly scalable and resilient applications.
- Administer and optimise Kubernetes clusters on AWS, employing advanced orchestration techniques to manage containerised workloads.
- Analyse, evaluate, and mitigate security vulnerabilities within Kubernetes deployments on AWS, implementing robust protective measures.

- Design, implement, and justify robust AWS solution architectures, ensuring cost-effective, scalable, and secure cloud infrastructures.
- Administer and manage Microsoft Azure environments, implementing comprehensive solutions across resource management, virtual networking, identity access, data storage, operational continuity, recovery, and cost optimisation.
- Formulate and apply integrated cloud security strategies across DevOps, SysOps, cybersecurity, and GRC domains to secure cloud-based assets and infrastructures.
- Critically review and apply cloud security principles and practices to ensure robust protection of data, applications, and infrastructure across diverse cloud platforms.
- Design, develop, and manage security architectures, evaluating alignment with organisational objectives and regulatory standards across the six critical ISSAP domains.
- Evaluate and implement Zero Trust Frameworks to enhance cloud assurance, strengthening overall cloud security postures and response strategies.

8. Who Should Enrol in this Program?

This Diploma in DevSysOps Engineering diploma is designed for:

- School, College and university students looking to gain admissions in the third year. of Bachelor's degree globally and expand their knowledge, skills, and career opportunities as well.
- Individuals looking to learn job based skills and secure employment globally.
- Professionals in the industry who want to enhance their skills and advance their careers.

This diploma program is suitable for individuals between the ages of 16 and 45 who are self-motivated and capable of studying independently. The diverse student body, composed of individuals from various industries and backgrounds, enriches class discussions and interactions.

The diploma prepares individuals for careers such as:

- SysOps Administrator, Cloud Solutions Architect, Cloud Security Engineer
- AWS Certified Solutions Architect, AWS Certified DevOps Engineer, AWS Certified SysOps Administrator, Security Compliance Analyst
- Cybersecurity Analyst, Cloud Security Specialist, Cloud Compliance Analyst
- Security Engineer, Cloud DevSecOps Engineer, DevOps Security Engineer
- AWS Security Consultant, AWS Cloud Compliance Manager, Cloud Security Architect, DevSecOps Specialist
- Network Security Engineer, Incident Response Analyst, Cloud Penetration Tester
- AWS Cloud Security Specialist, DevSecOps Consultant, AWS Security Specialist
- Docker Administrator, Automation Engineer, Deployment Engineer, Secure Software Developer
- Security Governance Analyst, Security Risk Manager
- DevSecOps Consultant, Cloud Security Consultant
- Cybersecurity Operations Manager, Security Assessment Specialist
- Compliance and Risk Analyst, Cloud Security Compliance Manager
- Cloud Security Operations Manager, Security Analyst Engineer
- DevSecOps Automation Engineer, DevOps Engineer, System Administrator

- Cloud Risk Analyst, Security Solutions Architect
- Ansible Engineer, Infrastructure Engineer, Cloud Security Operations Analyst
- JIRA Administrator, Python Developer, Security Automation Engineer
- Kubernetes Administrator, Cloud Engineer, Deployment Engineer
- Kubernetes Developer, Application Developer
- Kubernetes Security Engineer, Security Specialist, DevSecOps Engineer
- Python Developer, Automation Engineer, Data Analyst
- Selenium Automation Engineer, Software Developer, Web Application Developer
- Data Analyst, Data Scientist, Machine Learning Engineer
- SOC Engineer, Threat Hunting Engineer
- Ethical Hacker, Incident Response Manager, Security Analyst
- Information Security Manager, Security Consultant, Security Auditor
- Job seeker, Professional looking to improve their LinkedIn profile
- Linux Administrator, System Administrator, DevOps Engineer
- Network Security Analyst, Penetration Tester, Ethical Hacker
- PCI DSS Compliance Auditor, Compliance Officer
- Python Developer, App Developer
- SCADA Security Analyst, Cyber Security Consultant
- SIEM Engineer, Security Operations Center (SOC) Analyst
- Vulnerability Assessment Specialist, Penetration Tester

9. Learning Path

1. Linux Deep Dive
2. Python Deep Dive
3. Red Hat Enterprise Linux (RHEL)
4. Certified Information System Security Professional (CISSP)
5. AWS Solution Architecture
6. Python Automation
7. Certified Kubernetes Application Developer (CKAD)
8. Certified Kubernetes Administrator (CKA)
9. Ansible Deep Dive
10. DevOps Docker Deep Dive
11. Certificate of Cloud Security Knowledge (CCSK)
12. Certified Kubernetes Security Specialist (CKS)
13. Python Flask
14. Python Selenium
15. Docker Deep Dive I
16. Bash Script Deep Dive I
17. Python Automation Deep Dive I
18. Python Selenium I
19. JIRA with Python I
20. Python Flask I
21. Vagrant I
22. Ansible I
23. Kubernetes Application Developer I
24. Kubernetes and Cloud Native Associates I

25. Kubernetes Administrator I
26. Kubernetes Security Specialist I
27. AWS Solution Architecture I
28. Microsoft Azure Administrator I
29. Professional Cloud Security I
30. Cloud Security Standards Review I
31. ISSAP Architecture Professional Review I
32. Cloud Assurance_ Zero Trust Frameworks
33. LinkedIn Course for Job Seekers
34. IELTS Academic and General Training
35. Pass all MCQs and all AI Razzaq part 1 labs given for the diploma
36. Achieve a 6.5 band or more in IELTS for UKVI
37. Attain EduQual Certificate.

10. Assessment Information

Assessments are an essential component of any diploma course, and at our online and distance learning platform, we ensure that our students are evaluated thoroughly. This section outlines the assessment framework specifically designed for students who enroll in their EduQual diploma programs from July 2026 onwards.

10.1. Assessment Overview

Student assessments are designed to provide practical, skills-based learning experiences that reflect real-world vocational requirements across emerging technology domains.

Assessment Components

Assessment Component	Weightage	Passing Percentage Requirement
AI Razzaq Lab Assignments(part 1 only)	70%	Minimum 40%
Multiple Choice Questions (MCQs)	15%	Minimum 40%
English Language Exam	15%	Minimum IELTS 6.5 or Duolingo 115–120

Important: You must achieve a minimum of 40% in each of the AI Razzaq Lab Assignments(part 1) and MCQs exam to qualify for diploma completion. Students will have to pay for IELTS for UKVI on their own. The fee is not included in the diploma fee.

10.2. AI Razzaq Lab Assignments (70% weightage in overall Grade)

What Are They?

AI Razzaq Lab Assignments are practical, hands-on tasks divided into three phases:

Phase	Description
Basic Phase	Foundational tasks introducing core concepts and tools
Intermediate Phase	Integrated tasks requiring application of skills in scenario-based contexts
Advanced Phase	Complex, multi-step tasks simulating real-world problem-solving

These assignments are customized based on your chosen emerging technology domain (e.g., AIOps, DevSysOps, DevOps, SysOps, Cloud Advancement).

How Are They Graded?

- Assignments are submitted via the student portal.
- Graded using AI-augmented assessment tools.
- Students receive real-time feedback on their performance
- Final scores are recorded as a percentage

What If You Need to Resubmit?

Scenario	Process
First failure	You may resubmit once within 30 days of receiving your result
Second failure	You must repeat the unit with full attendance and reassessment of all phases
Lab access expires before completion	You must renew access as per the Course Access Policy
Lab assessments incomplete within two years	£100 reassessment fee applies

10.3. Multiple Choice Questions (15% of Your Grade)

Assessment Format

- Each MCQ carries 1 mark

- No negative marking for incorrect answers
- Questions include:
 - Knowledge-based
 - Scenario-based
 - Job-based
 - Critical Thinking
 - Application-based

Attempts and Scoring

Feature	Detail
Attempts	Unlimited attempts within your program access period
Final Score	Average of all attempts that meet or exceed the passing grade
Passing Requirement	Minimum 40%
Requirement	You must pass each individual assessment bank (20 MCQs each)

Diploma Program Access Period

Diploma Level	Access Period
EduQual Level 3 & 4	12 months (in total)
EduQual Level 5	15 months (in total)
EduQual Level 6	18 months (in total)

Note: If you fail to complete all MCQ assessments within your program access period, you must renew access as per the Course Access Policy.

10.4. English Language Exam (15% of Your Grade)

Mandatory Requirement

You must appear for IELTS for UKVI and score a 6.5 band or more to complete the minimum requirements of the exam.

Submission Requirements

You must submit:

- Official score report (verified link or Test Report Form)
- Valid identification matching test records

- Test date (must be within 2 years)
- Registered email used for the test

All submissions must be uploaded via the AI Nafi Student Portal or verified directly through official providers.

Verification and Compliance

AI Nafi International College reserves the right to verify scores with official test providers. Non-compliance or falsification will result in academic disciplinary action and possible program suspension or termination.

Why Is This Required?

Submission of a valid English proficiency score is required for:

- Program completion and diploma issuance
- Participation in AI Razzaq Program (employment pathways)
- Eligibility for international university admissions or work based opportunities

If you do not meet the minimum requirement, you must retake the test until the required benchmark is achieved and participate in mandatory live classes of IELTS happening weekly.

10.5. AI Razzaq Labs Program Access

Prerequisites for Lab Access

Access to AI Razzaq Labs requires completion of:

1. Enrollment in an eligible EduQual diploma program (Levels 3 to 6)
2. Know Your Student (KYS) Form submission, capturing:
 - Academic background
 - Career goals
 - Geographic preferences
 - Industry focus
3. Engagement with the program as per your selected study plan (monthly, quarterly, annual)

Lab Components

Component	Description
Course-Linked Labs	Embedded and mandatory labs directly tied to your diploma coursework
KYS-Based Personalized Labs	Customized labs tailored to your individual career and skill profile

Additional Features and Support

Every learner will benefit from:

Feature	Description
AI-Driven Internship Guidance	Personalized internship recommendations and preparation
Resume Building	ATS scoring and career coaching
Interview Preparation	AI-powered voice interview practice (coming soon)
GitHub Integration	Portfolio building and code repository integration
Skill Certification Badges	Recognition of completed competencies
Global Career Forum	Access to networking and opportunities
University Admission Assistance	Support for university applications worldwide
Visa and Work Permit Support	Assistance for 70+ countries and G20 nations
Post-Employment Services	30, 60, and 90-day post-employment support
Job Placement	Placement assistance with Fortune 500 and global companies

10.6. Grading Criteria

Final grade is determined by applying the weightage of each assessment component to the scores a student achieves. Each component's score is multiplied by its respective weightage, and the results are summed to calculate your overall grade.

Grades are awarded based on absolute grading criteria, meaning the final grade depends solely on the performance against the predefined percentage thresholds, rather than being compared to other students.

Grade Boundaries

Grade	Percentage Range
A*	90% and above

A	80% – 89%
B	70% – 79%
C	60% – 69%
D	50% – 59%
U	Below 50%

Example Calculation

For a student:

Component	Score Achieved	Weightage	Weighted Score
Lab Assignments	75%	× 70%	= 52.5%
MCQs	60%	× 15%	= 9.0%
English Exam	65%	× 15%	= 9.75%
Final Grade			71.25%

A final score of 71.25% would correspond to a Grade B.

IELTS Band Score to Percentage Conversion

The IELTS test does not have a direct, official percentage conversion. However, for the purpose of diploma, the minimum requirement is Band 6.5, and any score above 6.5 is considered as meeting and exceeding the requirement.

What Does a Band 7 Mean?

A Band 7 indicates a student is a “Good User” of English. According to IELTS:

“You have an operational command of the language, though with occasional inaccuracies, inappropriacies and misunderstandings in some situations. You generally handle complex language well and understand detailed reasoning.”

How Is Band 7 Treated for Diploma?

For English Language Exam component (15% of overall grade), the scoring works as follows:

IELTS Band	Status	Percentage Equivalent (for grading purposes)
Below 6.5	Fail	0% – Does not meet the minimum requirement

6.5	Pass (Minimum)	50%
7.0	Pass (Good)	Approximately 75%
7.5	Pass (Very Good)	Approximately 85%
8.0+	Pass (Excellent)	100%

How English Score Affects Final Grade

Since the English Exam contributes 15% to overall grade, here is how a Band 7 (≈75%) contributes:

Component	Student Score	Weightage	Weighted Contribution
English Exam	75%	× 15%	= 11.25% (out of 15%)

Example: Overall Grade Calculation

Component	Your Score	Weightage	Weighted Score
Lab Assignments	70%	× 70%	= 49.00%
MCQs	60%	× 15%	= 9.00%
English Exam	75% (Band 7)	× 15%	= 11.25%
Final Grade	C		69.25%

A final score of 69.25% would correspond to a Grade C.

Quick Reference Table

IELTS Band	Interpretation	Approx. Percentage	Weighted Contribution (15%)
6.5	Minimum Pass	50%	7.5%

7.0	Good User	75%	11.25%
7.5	Very Good User	85%	12.75%
8.0+	Excellent User	100%	15.00%

Note: The percentage equivalents above are used only for the purpose of calculating your overall diploma grade. They do not represent an official IELTS percentage conversion, as IELTS does not provide one. Any score of 6.5 or above satisfies the English proficiency requirement for your diploma.

10.7. Academic Integrity

To maintain academic integrity, the following practices are strictly prohibited:

Prohibited Practice	Description
Use of Automated Tools	Employing bots, scripts, or unauthorized software to answer MCQs or manipulate assessment platforms
Undisclosed AI-Generated Work	Passing off AI-created content as original work without proper acknowledgment or authorization
Unauthorized Assistance	Using prohibited tools, devices, or receiving help during practical exams

Violation Response

If suspected malpractice is detected:

1. Student will be formally informed in writing
2. A panel will review the evidence
3. Student will have the opportunity to respond
4. If confirmed, student may be banned from retaking the assessment and may be disqualified from the diploma program

10.8. Support for Students

The college provides comprehensive support to help students succeed:

Support Type	Description
Academic Integrity Workshops	Sessions on plagiarism prevention and ethical assessment practices
Counseling and Advising	Guidance on academic challenges and career planning
Detailed Feedback	Constructive feedback on assessments to guide improvement
AI Usage Guidance	Resources on responsible AI usage in academic work
Technical Support	Assistance with platform and technical issues via live chat or email

10.9. Accessibility and Reasonable Adjustments

The college is committed to ensuring equal access to assessments. If students have documented disabilities or special needs, they may request reasonable adjustments, including:

- Extra time
- Alternative formats
- Assistive technology
- Modified lab environments

Submit requests to: academics@alnafi.com

Timeline: At least 7 working days before the scheduled assessment with supporting documentation.

10.10. Appeals Process

If any student believes an assessment decision is unfair:

Step	Timeline	Action
Informal Review	Within 10 working days of receiving results	Contact academics@alnafi.com
Formal Appeal	Within 14 working days of informal response	Submit formal appeal with supporting evidence

Acknowledgment	Within 3 working days	Appeal is acknowledged and assigned for review
Final Decision	Within 15 working days	Impartial panel issues final written decision

Complete Course Units

Unit 1: Linux Deep Dive

Unit Objectives:

- Build comprehensive Linux system administration skills
- Master installation, configuration, and management
- Develop security, networking, and monitoring expertise
- Learn automation and high availability concepts

Unit Curriculum:

- Introduction and installation (virtual environment, custom partitions, hardening)
- Basic configuration (system architecture, commands, file systems, permissions)
- Bash shell scripting
- Package management with YUM/DNF
- Advanced Linux configuration (single-user mode, run levels, performance reporting)
- Linux networking (DHCP, static/dynamic IP, DNS, routing)
- Advanced disk management (partitions, LVM, file systems)
- Linux services (SSH, NFS, Samba, NTP, cron)
- Linux security (firewalld, iptables, rkhunter)
- Web, MySQL, and Squid server configuration
- High availability (bonding, teaming, failover, load balancing)
- Linux monitoring (Nagios, NRPE, Docker monitoring)
- AI-powered automation and optimization

Unit 2: Python Deep Dive

Unit Objectives:

- Build deep, professional Python programming skills
- Master OOP, data structures, and advanced features
- Develop web applications, APIs, and data solutions
- Implement testing, debugging, and best practices

Unit Curriculum:

- Introduction to Python environment and setup
- Basic syntax and operations
- Data structures (lists, tuples, dictionaries, sets, strings)
- Modules and packages
- Object-Oriented Programming (classes, inheritance, polymorphism)
- Advanced topics (decorators, generators, context managers)

- Working with data (CSV, JSON, databases, Pandas)
- Web development (Flask, Django, RESTful APIs)
- Testing and debugging (unit tests, TDD)
- Concurrency and parallelism (threading, multiprocessing, asyncio)
- Network programming (sockets, client-server)
- Advanced libraries and tools (regex, logging, argparse)
- Best practices and design patterns (PEP 8)
- Python 3.13 new features
- Capstone project

Unit 3: Certified Information Systems Security Professional (CISSP)

Unit Objectives:

- Prepare learners for the CISSP certification exam
- Master all domains of the CISSP Common Body of Knowledge
- Develop expertise in security governance, risk management, and operations
- Build comprehensive understanding of security technologies and practices

Unit Curriculum:

- Security governance through principles and policies
- Personnel security and risk management concepts
- Business continuity planning
- Laws, regulations, and compliance
- Protecting security of assets
- Cryptography and symmetric key algorithms
- PKI and cryptographic applications
- Security models, design, and capabilities
- Security vulnerabilities, threats, and countermeasures
- Physical security requirements
- Secure network architecture and components
- Secure communications and network attacks
- Managing identity and authentication
- Controlling and monitoring access
- Security assessment and testing
- Managing security operations
- Preventing and responding to incidents
- Disaster recovery planning
- Investigations and ethics
- Software development security
- Malicious code and application attacks

Unit 4: Red Hat Enterprise Linux (RHEL)

Unit Objectives:

- Install, configure, and manage Red Hat Enterprise Linux systems

- Implement security, networking, and storage solutions
- Master automation with Shell and Ansible
- Manage containers and virtualization

Unit Curriculum:

- RHEL 9 overview and architecture
- Installation and initial setup
- Linux fundamentals and shell
- Software management with DNF/YUM
- User and access control
- Storage and file systems
- Networking and remote access
- Security and SELinux
- Monitoring and performance
- Automation with Shell and Ansible
- Containers and Podman
- Virtualization and high availability

Unit 5: AWS Solutions Architect

Unit Objectives:

- Design secure access controls to AWS resources using IAM, MFA, and federated access.
- Architect resilient, highly available, and fault-tolerant systems across multiple Availability Zones.
- Optimize high-performance storage, compute, and database solutions for scalable cloud workloads.
- Implement cost-effective architectures by selecting appropriate pricing models and storage lifecycles.
- Evaluate and apply security best practices for VPC, encryption, and incident response.

Unit Outline:

- Module 1: Design Secure Architectures – Secure access to AWS resources, IAM fundamentals, users, groups, roles, policies, MFA best practices, STS and role switching, cross-account and federated access, AWS SSO, Control Tower and SCPs, resource-based policies, VPC security basics, security groups, NACLs, route tables, public/private subnet design, NAT gateways, bastion hosts, AWS Shield and WAF, AWS Secrets Manager, VPN and Direct Connect, data encryption in transit and at rest, ACM and TLS, encryption key management, backup, replication, DR planning, regulatory compliance.
- Module 2: Design Resilient Architectures – Scalable and loosely coupled architectures, event-driven, microservices, and multi-tier patterns, horizontal and vertical scaling strategies, loose coupling techniques, containers and serverless architectures, selecting compute/storage/networking/database services, high availability concepts and AWS service choices, fault tolerance across AZs and regions, infrastructure automation (Auto Scaling, CloudFormation), monitoring and health checks, data durability strategies, DR planning and AWS DR solutions, modernizing legacy applications.
- Module 3: Design High-Performance Architectures – Amazon S3, EBS, and EFS features and use cases, hybrid storage architectures, storage scalability and optimization, decoupling workloads, Auto Scaling metrics and triggers, EC2 instance types and sizes,

compute alternatives (on-demand, reserved, spot, serverless), Amazon RDS, Aurora, DynamoDB performance features, read replicas and caching strategies, capacity planning, database engine selection, global/hybrid/multi-tier network architectures, CloudFront and Global Accelerator, load balancing options, network resource placement, data lakes, Kinesis, Data Firehose, data transfer and transformation services, visualization and analytics.

- Module 4: AWS Cost Optimization – Storage class selection and lifecycle policies (S3 Standard, Glacier, etc.), Cost Explorer, Budgets, optimizing storage size and access frequency, cost-effective backup and archiving, data migration services and cost considerations, pricing models and instance purchase options, cost-effective Auto Scaling and load balancing, selecting instance families for budget efficiency, balancing performance and cost.
- Module 5: Design Cost-Effective Architectures – Database backup and retention cost optimization, cost-effective database engines and services, replication and capacity planning cost management, efficient database migration, cost-effective network topologies, NAT gateway and VPN cost optimization, network routing and peering for cost reduction, CDN usage and edge caching strategies, monitoring network costs and optimizing bandwidth usage.

Unit 6: Python Automation

Unit Objectives:

- Design Python automation scripts for file operations and data processing.
- Implement web scraping and browser automation solutions.
- Apply API automation for testing and interaction.
- Design cloud infrastructure automation and workflow automation solutions.
- Implement task scheduling, monitoring, and reporting systems.

Unit Course:

- Module 1: Introduction to Python for Automation – Overview, setup, Python scripting.
- Module 2: Automating System – System administration, process automation.
- Module 3: Automating Web Scraping – Introduction, data extraction and storage.
- Module 4: Automating Testing – Unit to integration testing, API testing, CI integration.
- Module 5: Automating Web Interactions – Browser automation with Selenium.
- Module 6: Automating API Interactions – Making and testing API requests.
- Module 7: Automating Cloud Infrastructure – Azure and GCP automation.
- Module 8: Task Scheduling and Workflow Automation – Cron scheduling, workflow automation, building pipelines.
- Module 9: Monitoring Automated Tasks – Monitoring, reporting, error handling.
- Module 10: Best Practices – Maintainable code, security, performance optimization.

Unit 7: Certified Kubernetes Application Developer (CKAD)

Unit Objectives:

- Design and build containerized applications for Kubernetes deployment.
- Utilize appropriate workload resources and multi-container pod design patterns.

- Implement application deployment strategies including blue/green and canary deployments.
- Apply observability, monitoring, and debugging techniques for applications.
- Configure application security, environment configuration, services, and networking.

Unit Course:

- Module 1: Application Design and Build – Container images, workload resources (Deployment, DaemonSet, CronJob), multi-container pod design patterns, storage options, AI-driven container orchestration.
- Module 2: Application Deployment – Deployment strategies (blue/green, canary), rolling updates, Helm package manager, Kustomize, AI-powered deployment automation.
- Module 3: Application Observability and Maintenance – API deprecations, probes and health checks, monitoring with CLI tools, container logging, debugging techniques, AI-driven predictive monitoring.
- Module 4: Application Environment, Configuration, and Security – Extending Kubernetes with CRDs and Operators, authentication/authorization, resource management, configuration management with ConfigMaps and Secrets, security best practices, AI-driven security automation.
- Module 5: Services and Networking – Network policies, application access via services (ClusterIP, NodePort, LoadBalancer), Ingress rules, AI-powered network traffic analysis.

Unit 8: Certified Kubernetes Administrator (CKA)

Unit Objectives:

- Deploy, manage, and troubleshoot Kubernetes clusters in production environments.
- Design storage solutions using Persistent Volumes and StorageClasses.
- Apply troubleshooting techniques for applications, nodes, clusters, and networking.
- Implement workload management, deployment strategies, and scheduling.
- Configure cluster architecture, installation, upgrades, and networking services.

Unit Course:

- Module 1: Storage – StorageClasses, Persistent Volumes, volume modes, access modes, reclaim policies, Persistent Volume Claims, configuring applications with persistent storage, AI-powered predictive storage optimization.
- Module 2: Troubleshooting – Cluster and node logging, application monitoring, managing container logs, troubleshooting application failures, cluster component failures, networking issues, AI-assisted autonomous troubleshooting.
- Module 3: Workloads & Scheduling – Deployments, rolling updates, rollbacks, ConfigMaps and Secrets, scaling applications, self-healing, pod scheduling, resource limits, manifest management, AI-driven intelligent workload scheduling.
- Module 4: Cluster Architecture, Installation & Configuration – RBAC management, installing Kubernetes with Kubeadm, managing highly available clusters, provisioning infrastructure, upgrading clusters, etcd backup and restore, AI-driven cluster health optimization.
- Module 5: Services & Networking – Host networking configuration, pod-to-pod connectivity, service types, Ingress controllers and resources, CoreDNS configuration, choosing a CNI, AI-powered network traffic optimization.

Unit 9: Ansible Deep Dive

Unit Objectives:

- Design and implement infrastructure automation solutions using Ansible.
- Utilize Ansible Playbooks, Ad-Hoc Commands, and Roles for configuration management.
- Apply variables, facts, conditional logic, and loops in automation scripts.
- Implement provisioning, networking, and cloud deployments using Ansible.
- Integrate Ansible with CI/CD pipelines and apply security best practices.

Unit Course:

- Module 1: Introduction to Ansible – Definition, purpose, benefits, architecture, YAML, environment configuration.sk
- Module 2: Ansible Basics for Developers – Playbooks, ad-hoc commands, variables, facts, conditional logic, inventory management.
- Module 3: Ansible for Administrators – Static vs dynamic inventory, managing users/packages/services, file management, Jinja2 templates, roles.
- Module 4: Advanced Ansible for Developers – Loops, conditions, handlers, multi-environment management, Ansible Vault, cloud provisioning.
- Module 5: Ansible Automation for Administrators – Network device configuration, database automation, Ansible Tower/AWX, collections, debugging and troubleshooting.
- Module 6: Ansible Advanced Concepts – Idempotent and scalable playbooks, Git integration, CI/CD, security and compliance, AWS automation.
- Module 7: Best Practices – Automating full stack deployments, CI/CD pipeline integration, real-world case studies.

Unit 10: DevOps Docker Deep Dive

Unit Objectives:

- Analyze Docker components and containerization principles.
- Integrate Docker with DevOps tools and workflows.
- Design Docker images and manage container repositories.
- Implement container orchestration using Docker Swarm.
- Apply security best practices for Docker containers.

Unit Course:

- Module 1: Introduction – Security principles, threat landscape, security in CI/CD, containers, microservices.
- Module 2: Docker Fundamentals – Container environments, installation, architecture, managing containers.
- Module 3: Docker Images & Repositories – Building images, Dockerfiles, build process, registries, Docker Compose, volumes.
- Module 4: Docker Configuration Management – DevOps repositories, branching strategies, Git integration, excluding files, multi-stage builds.
- Module 5: Docker Orchestration – Orchestration concepts, Docker Swarm, Swarm vs Kubernetes.
- Module 6: DevOps & Docker – DevOps evolution, tools, Ansible integration.
- Module 7: Security & Docker – Security architecture, least privilege, content trust, network security, best practices.

Unit 11: Certificate of Cloud Security Knowledge (CCSK)

Unit Objectives:

- Define cloud computing concepts, deployment models, and service models.
- Apply cloud governance strategies, risk management, and compliance frameworks.
- Secure cloud infrastructure, networks, workloads, and data using shared responsibility models.
- Implement identity and access management, security monitoring, and incident response.
- Evaluate related technologies such as Zero Trust, AI, and SASE for cloud security.

Unit Outline:

- Domain 1: Cloud Computing Concepts & Architecture – Defining cloud computing, abstraction and orchestration, essential characteristics, cloud service models (IaaS, PaaS, SaaS), cloud deployment models, CSA Enterprise Architecture Model, shared security responsibility model.
- Domain 2: Cloud Governance and Strategies – Cloud governance, governance hierarchy, aligning with requirements and standards, consulting with stakeholders, cloud security frameworks, Cloud Controls Matrix (CCM), CSA STAR Registry, policies.
- Domain 3: Risk, Audit and Compliance – Cloud risk management, cloud risks, corporate risk management strategy, risk assessment and treatment, assessing cloud services, business requests, review CSP documentation, compliance and audit, jurisdictions, privacy laws and regulations, compliance inheritance, artifacts of compliance, GRC tools and technologies.
- Domain 4: Organization Management – Organization hierarchy models, capabilities within a CSP, building hierarchy, managing organization-level security, identity provider and user/group/role mappings, shared services, hybrid and multi-cloud deployments, tooling and staffing.
- Domain 5: Identity and Access Management – How IAM is different in the cloud, fundamental terms, federation, common federation standards, federated identity management, managing users and identities.
- Domain 6: Security Monitoring – Cloud monitoring, logs and events, posture management, management plane logs, service and application logs, resource logs, cloud-native tools, telemetry sources, collection architectures, log storage and retention, cascading log architecture, AI for security monitoring.
- Domain 7: Infrastructure & Networking – Cloud infrastructure security techniques, CSP infrastructure responsibilities, infrastructure resilience, cloud network fundamentals, SDN-based components, cloud connectivity, preventative and detective security measures, Infrastructure as Code (IaC), Zero Trust, Software Defined Perimeter (SDP), ZTNA, SASE.
- Domain 8: Cloud Workload Security – Types of cloud workloads, securing virtual machines, challenges and mitigations, secure VM images, snapshots, securing containers, container image creation and networking, container orchestration security, runtime protection, securing serverless and FaaS, IAM for serverless, securing AI workloads.
- Domain 9: Data Security – Cloud storage primer (object, block, database), data classification, IAM, access policies, encryption and key management, DLP, cloud data encryption at rest, application level encryption, key management strategies (client-side, server-side, customer-managed), KMS, Data Security Posture Management (DSPM).
- Domain 10: Application Security – Secure Development Lifecycle (SSDLC), threat modeling, pre-deployment and post-deployment testing, architecture's role in security,

identity and access management for applications, secrets management, DevOps and DevSecOps, CI/CD pipelines, WAFs and API gateways.

- Domain 11: Incident Response & Resilience – Incident response lifecycle, preparation, detection and analysis, cloud system forensics, container and serverless forensics, containment, eradication, recovery, post-incident analysis.
 - Domain 12: Related Technologies & Strategies – Zero Trust technical objectives and pillars, Zero Trust and cloud security, AI workloads and cloud security intersection.
-

Unit 12: Certified Kubernetes Security Specialist (CKS)

Unit Objectives:

- Implement security best practices for Kubernetes clusters at all levels.
- Design cluster hardening, system hardening, and network security strategies.
- Analyze and minimize microservice vulnerabilities throughout the supply chain.
- Implement monitoring, logging, and runtime security solutions.
- Evaluate and apply AI-driven security solutions in Kubernetes environments.

Unit Course:

- Module 1: Cluster Setup – Implementing network security policies, CIS benchmark security review, Ingress security with TLS, node metadata protection, verifying platform binaries, AI-driven security posture management.
 - Module 2: Cluster Hardening – RBAC for minimal exposure, service account security, Kubernetes API access restrictions, version upgrades for vulnerability mitigation, AI-powered anomaly detection.
 - Module 3: System Hardening – Minimizing host OS footprint, least-privilege IAM, restricting external network access, kernel hardening with AppArmor/seccomp/SELinux, AI-driven threat detection.
 - Module 4: Minimizing Microservice Vulnerabilities – Pod Security Standards, managing Kubernetes Secrets securely, isolation techniques for multi-tenancy, pod-to-pod encryption with Cilium, AI-powered security and threat response.
 - Module 5: Supply Chain Security – Minimizing base image footprint, understanding software supply chain, SBOM, image signing and verification, static analysis of images, AI-driven threat detection.
 - Module 6: Monitoring, Logging, and Runtime Security – Behavioral analytics for threat detection, threat detection across infrastructure, attack investigation, container immutability, Kubernetes audit logs, AI-driven security automation.
-

Unit 13: Python Flask

Unit Objectives:

- Design and develop web applications using Flask framework.
- Implement routing, templating, and request/response handling.
- Integrate databases using SQLAlchemy and manage migrations.
- Apply authentication, authorization, and error handling.
- Implement testing, deployment, and advanced features like caching and WebSockets.

Unit Course:

- Module 1: Introduction to Flask – Overview, features, installation, first application, WSGI.
- Module 2: Flask Application Basics – Structure, development server, app/request context, debug mode.
- Module 3: Routing and URL Building – Defining routes, variables, url_for, HTTP methods.
- Module 4: Templates and Rendering – Jinja2, render_template, template inheritance, data passing.
- Module 5: Handling Requests and Responses – Request object, form data, cookies, sessions, custom responses.
- Module 6: Flask Extensions and Database Integration – SQLAlchemy, Migrate, WTForms.
- Module 7: Authentication and Authorization – Login/logout, Flask-Login, role-based access, error handling.
- Module 8: Advanced Topics – Blueprints, application factory, testing, deployment, Celery, caching, WebSockets, REST APIs.

Unit 14: Python Selenium

Unit Objectives:

- Design web automation solutions using Python Selenium.
- Implement Selenium WebDriver scripts for web element identification.
- Apply synchronization techniques and advanced user interactions.
- Analyze and debug automation scripts effectively.
- Utilize automation frameworks like Page Object Model (POM).

Unit Course:

- Module 1: Introduction – Introduction to Selenium, setting up WebDriver, AI-driven foundations.
- Module 2: Identification of Web Elements – Finding elements by ID, name, class, CSS, XPath, link text, tag name, AI-powered techniques.
- Module 3: Handling Multiple Web Elements – Locating multiple elements, find_elements_by_* methods, AI-driven scalable identification.
- Module 4: Synchronization in Selenium – Implicit waits, explicit waits, intelligent synchronization.
- Module 5: Advanced User Interaction Automation – Action Chains, click_and_hold, context_click, drag_and_drop, key_down, move_to_element, send_keys.
- Module 6: Advanced Selenium WebDriver Techniques – Special keys, handling alerts, cookies, navigation, assertions, optimization, debugging.
- Module 7: Automation Frameworks – Page Object Model (POM), browser automation, AI-enhanced frameworks.

Unit 15: Docker Deep Dive I

The course "Docker Deep Dive I" offers an in-depth exploration of the integration of Amazon Web Services (AWS) with Docker containers. This course equips learners with the practical skills and knowledge necessary to effectively provision, configure, deploy, monitor, secure, and manage

containerized applications within AWS cloud infrastructure. It emphasises best practices in DevOps and containerization, ensuring that learners are well-prepared for real-world scenarios.

Key Learning Objectives

Upon completing this course, learners will be proficient in the following key areas

- Provisioning and configuring AWS EC2 instances suitable for Docker deployments.
- Creating Docker images and storing them on AWS Elastic Container Registry (ECR).
- Deploying Docker containers on AWS Elastic Container Service (ECS).
- Implementing continuous integration by automatically building Docker images when code changes occur.
- Automating deployment changes to ECS using Docker.
- Understanding Docker's networking capabilities within the AWS environment.
- Implementing persistent storage solutions for Docker containers using AWS services.
- Setting up and managing Docker Swarm clusters on AWS.
- Implementing effective monitoring and logging for Docker containers using AWS CloudWatch.
- Applying best practices for securing Docker containers on AWS.

Course Curriculum

- Lesson 1: Setting up an AWS EC2 Instance for Docker
- Lesson 2: Building a Basic Docker Image and Pushing to AWS Elastic Container Registry (ECR)
- Lesson 3: Running Docker Containers on AWS Elastic Container Service (ECS)
- Lesson 4: Implementing Continuous Integration with AWS CodeBuild and Docker
- Lesson 5: Continuous Deployment with AWS CodePipeline, ECS, and Docker
- Lesson 6: Docker Networking on AWS
- Lesson 7: Docker Volumes and Storage on AWS
- Lesson 8: Implementing Docker Swarm on AWS
- Lesson 9: Monitoring Docker Containers with Amazon CloudWatch
- Lesson 10: Advanced Security with Docker and AWS

Unit 16: Bash Script Deep Dive I

This course delves into the intricacies of setting up AWS EC2 instances for Bash and Docker work, providing students with hands-on experience in cloud-based development and containerization.

Key Learning Objectives

Upon completing this course, learners will develop proficiency in the following key areas:

- Provisioning and Configuring AWS EC2 Instances: Students will acquire the skills to provision and configure AWS EC2 instances optimised for Docker deployments.

- **Creating Docker Images:** The course will teach students how to create Docker images and effectively store them on AWS Elastic Container Registry (ECR).
- **Deployment Strategies:** learners will gain an understanding of various deployment strategies, ensuring they can confidently select and implement the most suitable approach for specific scenarios.
- **Bash Scripting Mastery:** Students will become proficient in Bash scripting, learning how to automate Docker-related tasks effectively.

Course Curriculum

- Lesson 1: Setting up AWS EC2 for Bash and Docker Work
- Lesson 2: Basic Bash Script with Docker
- Lesson 3: Conditional Bash Scripts with Docker
- Lesson 4: Bash Loops with Docker Image Management
- Lesson 5: Accepting User Inputs for Docker Operations
- Lesson 6: Functions in Bash for Modular Docker Scripts
- Lesson 7: Scheduling Docker Workloads with Bash and Cron
- Lesson 8: Bash Scripting with AWS CLI and Docker
- Lesson 9: Advanced Bash Error Handling with Docker Operations
- Lesson 10: Continuous Deployment Script with Bash and Docker on AWS

Unit 17: Python Automation Deep Dive I

This course provides hands-on training in AWS cloud computing and Python scripting, focusing on automation and integration. learners will learn to set up AWS EC2 instances for Python development and create automation scripts to manage various AWS services. The course curriculum is designed to empower learners with practical skills in cloud infrastructure management and Python scripting.

Key Learning Objectives

Upon completing this course, learners will achieve proficiency in the following key areas:

- Setting up AWS EC2 for Python Development, including launching an EC2 instance, enabling SSH access, and installing Python and required packages using pip.
- Basic Python Scripting to Interact with AWS Services, encompassing the installation and configuration of Boto3 and the creation of Python scripts for listing AWS S3 buckets.
- Automating EC2 Instance Management with Python, covering scripting for starting/stopping EC2 instances and extending scripts for CPU utilisation monitoring.
- Python Automation for AWS RDS, involving the creation of RDS instances and Python scripts for manual backup triggers.
- Deploying Lambda Functions with Python, which includes writing Python Lambda functions and deploying them using AWS CLI or Boto3.
- Automating AWS S3 Operations with Python, focusing on scripting for uploading/downloading files from S3 and implementing versioning.

- Creating Dashboards on CloudWatch with Python, which encompasses generating CloudWatch metrics using Python and automating dashboard creation.
- Python Automation for AWS Elastic Load Balancing (ELB), including scripting ELB creation/configuration and traffic monitoring/analysis using Python.
- Event-driven Automation with AWS EventBridge and Python, covering the setup of EventBridge rules and the triggering of Python Lambda functions based on rule conditions.
- Infrastructure as Code (IaC) with AWS CDK and Python, involving the installation/configuring of AWS CDK and the development of AWS resource stacks using Python.
- Python Automation, which includes an introduction to Python and its installation, Python basics (commands, variables, data types, type casting, print formatting), working with various data structures, exception handling, file handling, database operations, and real-world project phases for web applications, data visualisation, and custom utilities.

Course Curriculum

- Lesson 1: Setting Up AWS EC2 for Python Development
- Lesson 2: Basic Python Scripting for AWS Interaction
- Lesson 3: Automating EC2 Instance Management with Python
- Lesson 4: Python Automation for AWS RDS
- Lesson 5: Deploying Lambda Functions with Python
- Lesson 6: Automating AWS S3 Operations with Python
- Lesson 7: Creating Dashboards on CloudWatch with Python
- Lesson 8: Python Automation for AWS Elastic Load Balancing (ELB)
- Lesson 9: Event-driven Automation with AWS EventBridge and Python
- Lesson 10: Infrastructure as Code (IaC) with AWS CDK and Python

Unit 18: Python Selenium I

Introduction

This course focuses on the practical application of Amazon Web Services (AWS) and Selenium automation for enhanced web development and testing capabilities. Learners will delve into various aspects of AWS integration and Selenium automation, gaining valuable skills and knowledge essential for modern software development and quality assurance.

Key Learning Objectives

Upon successful completion of this course, learners will attain proficiency in the following key areas:

- Setting up AWS EC2 for Selenium Development: learners will learn how to launch an AWS EC2 instance, establish SSH connections, and install Python, Selenium, and web drivers for Selenium-based automation tasks.

- Simple Web Automation Test: learners will create a basic Selenium script, navigate to websites, and capture webpage screenshots while grasping the fundamentals of Selenium automation.
- Using AWS S3 to Store Selenium Screenshots: learners will explore AWS S3 to create buckets and modify Selenium scripts to upload screenshots to these buckets, bridging AWS and Selenium.
- Automated Form Submissions: Learners will gain the ability to automate web form submissions using Selenium scripts, and store the results or responses on AWS RDS, enhancing data handling capabilities.
- Parallel Execution of Tests using Selenium Grid on AWS: learners will set up Selenium Grid Hub on EC2 instances, register multiple nodes with different browsers, and run test suites in parallel across these nodes.
- Continuous Integration with Jenkins and Selenium on AWS: This section covers the installation of Jenkins on EC2 instances, the creation of Jenkins jobs for Selenium tests, and the storage and review of test results, enabling seamless continuous integration.
- Monitoring Web Application Performance with Selenium and CloudWatch: learners will develop Selenium scripts to measure web page load times and push these performance metrics to AWS CloudWatch for monitoring.
- Error Reporting with Selenium and AWS SNS: Learners will modify Selenium scripts to detect test failures and integrate AWS SNS for timely notifications upon failures.
- Running Headless Selenium Tests on EC2: This module addresses the setup of necessary dependencies on EC2 instances and the execution of headless Selenium tests for efficient and resource-friendly automation.
- Scaling Selenium Tests using AWS Lambda and Step Functions: learners will configure AWS Lambda functions for running Selenium tests and orchestrate multiple tests using AWS Step Functions, achieving scalable and orchestrated test automation.
- Python Selenium Automation: This comprehensive section introduces learners to Python Selenium, covering installation, configuration, handling complex web elements, synchronisation, test automation using Pytest, and integration with Jenkins and GitHub for continuous testing.

Course Curriculum

- Lesson 1: Setting up AWS EC2 for Selenium Development
- Lesson 2: Simple Web Automation Test
- Lesson 3: Using AWS S3 to Store Selenium Screenshots
- Lesson 4: Automated Form Submissions
- Lesson 5: Parallel Execution of Tests using Selenium Grid on AWS
- Lesson 6: Continuous Integration with Jenkins and Selenium on AWS
- Lesson 7: Monitoring Web Application Performance with Selenium and CloudWatch
- Lesson 8: Error Reporting with Selenium and AWS SNS
- Lesson 9: Running Headless Selenium Tests on EC2
- Lesson 10: Scaling Selenium Tests using AWS Lambda and Step Functions

Unit 19: JIRA with Python I

Welcome to the course on "Jira Integration with Python." In this course, we will equip learners with the knowledge and skills required to seamlessly integrate Jira, a powerful project management and issue tracking tool, with Python. This integration will not only optimise processes but also enhance productivity in various domains such as DevOps, SysOps, Cloud Security, Cybersecurity, and Governance, Risk Management, and Compliance (GRC).

Key Learning Objectives

Upon successful completion of this course, you will be able to:

- Set up the Jira and Python environment, ensuring all the necessary components are in place for the upcoming labs.
- Learn the basics of Jira and how Python can be used to interact with Jira's API for essential tasks.
- Develop Python scripts to automate Continuous Integration/Continuous Deployment (CI/CD) pipeline notifications in Jira, streamlining the development workflow.
- Create Python scripts that integrate system alerts and notifications from monitoring tools into Jira, enhancing the efficiency of SysOps tasks.
- Develop Python scripts for detecting and reporting cloud security breaches in Jira, enhancing Cloud Security and Cybersecurity practices.
- Learn how to use Python and Jira to handle simulated cybersecurity threats effectively, preparing for real-world scenarios.
- Implement automation for governance, risk management, and compliance checks using Python and Jira, ensuring adherence to policies and regulations.
- Design Python scripts to automate audit log collection and reporting in Jira, enhancing transparency and accountability.
- Analyse and optimise Python scripts for better performance, security, and scalability.
- Reflect on and enhance the implemented solutions to ensure more efficient operations in the context of DevOps, SysOps, Cloud Security, Cybersecurity, and GRC.

Course Curriculum

- Lesson 1: Setting Up Jira and Python Environment
- Lesson 2: Basic Jira-Python Integration
- Lesson 3: Automate CI/CD Pipeline Notifications with Jira and Python
- Lesson 4: Monitoring SysOps Alerts with Python-Jira
- Lesson 5: Cloud Security Breach Detection with Jira
- Lesson 6: Automated Cybersecurity Threat Reporting
- Lesson 7: Governance and Compliance Checklist Automation
- Lesson 8: Automated Audit Log Collection and Reporting
- Lesson 9: Performance Optimization of Python-Jira Scripts
- Lesson 10: Reflection and Enhancement

Unit 20: Python Flask I

This course provides a comprehensive exploration of Amazon Web Services (AWS) and Flask development. Learners will engage in hands-on tasks and comprehensive documentation to develop practical skills in AWS and Flask.

Key Learning Objectives

Upon successful completion of this course, learners will attain proficiency in the following key areas:

- Setting up AWS EC2 for Flask Development: Learn to launch an EC2 instance, establish SSH connections, and install Python and Flask for web development.
- Developing a Simple Flask Application: Develop Flask routes and run a basic Flask app on an EC2 instance.
- Deploying Flask App with AWS Elastic Beanstalk: Prepare a Flask app for deployment and use Elastic Beanstalk to deploy it.
- Using AWS RDS with Flask: Create an RDS PostgreSQL instance and connect the Flask app to perform database operations.
- Implementing User Authentication in Flask using Amazon Cognito: Create a user pool in Cognito and implement authentication routes in Flask.
- Flask Application Monitoring with AWS CloudWatch: Integrate Flask logging with CloudWatch and set up alarms for specific events.
- Flask App CI/CD Pipeline with AWS CodePipeline and CodeDeploy: Store the Flask app in AWS CodeCommit and automate deployment using CodePipeline and CodeDeploy.
- Auto Scaling Flask Applications on AWS: Deploy the Flask app in an EC2 Auto Scaling group and set up scaling policies based on CloudWatch metrics.
- Implementing Flask API Caching using AWS ElastiCache: Create a Redis cluster in ElastiCache and modify the Flask app to cache API responses using Redis.
- Flask Application Security with AWS WAF and Shield: Set up AWS WAF with rules to filter malicious web traffic and implement AWS Shield for DDoS protection.

Course Curriculum

- Lesson 1: Setting up AWS EC2 for Flask Development
- Lesson 2: Developing a Simple Flask Application
- Lesson 3: Deploying Flask App with AWS Elastic Beanstalk
- Lesson 4: Using AWS RDS with Flask
- Lesson 5: Implementing User Authentication in Flask using Amazon Cognito
- Lesson 6: Flask Application Monitoring with AWS CloudWatch
- Lesson 7: Flask App CI/CD Pipeline with AWS CodePipeline and CodeDeploy
- Lesson 8: Auto Scaling Flask Applications on AWS
- Lesson 9: Implementing Flask API Caching using AWS ElastiCache
- Lesson 10: Flask Application Security with AWS WAF and Shield

Unit 21: Vagrant I

This course delves into the integration of Vagrant with Amazon Web Services (AWS) to facilitate efficient DevOps practices. learners will learn to set up Vagrant with AWS, enabling the creation and management of virtual machine environments for various tasks. The course encompasses key topics such as multi-machine environments, AWS RDS integration, provisioning scripts, AWS Elastic Load Balancing (ELB), Vagrant teardown and snapshots, AWS S3 storage utilisation, Vagrant networking with AWS, scalable Vagrant with AWS Auto Scaling Groups, and the conversion of Vagrant boxes into AWS AMIs.

Key Learning Objectives

Upon successful completion of this course, learners will achieve proficiency in the following essential areas:

- **Setting up Vagrant with AWS:** learners will master the installation of Vagrant and the AWS plugin, along with writing Vagrantfiles for EC2 instance provisioning, emphasising the significance of Vagrant in DevOps.
- **Multi-machine Environment with Vagrant:** Learners will update Vagrantfiles to include multiple VM definitions, exploring the design of multi-machine Vagrant environments.
- **Vagrant and AWS RDS Integration:** learners will learn to set up an RDS instance and configure EC2 instances for seamless communication with RDS.
- **Implementing Vagrant Provisioning Scripts:** This module covers writing shell scripts for installing web servers and applications, enabling their integration into Vagrant environments.
- **Vagrant and AWS Elastic Load Balancing (ELB):** Learners will create multiple EC2 instances using Vagrant and set up an AWS ELB for traffic distribution.
- **Vagrant Teardown and Snapshots:** This section explores Vagrant environment management, including halting, destroying, creating, and restoring from snapshots.
- **Vagrant and AWS S3 Storage:** learners will create S3 buckets and integrate AWS CLI into Vagrant provisioning scripts for interaction with S3.
- **Vagrant Networking with AWS:** Learners will configure private networking within Vagrantfiles, testing inter-VM communication within AWS environments.
- **Scalable Vagrant with AWS Auto Scaling Groups:** This module covers the setup of AWS Auto Scaling Groups and the deployment of Vagrant environments that can scale automatically.
- **Vagrant Boxes and AWS AMI:** learners will create customised EC2 instances using Vagrant, package them into Vagrant boxes, and convert these boxes into AWS AMIs.
- **Vagrant Tool Mastery for Managing Virtual Machine Environments:** Gain an in-depth understanding of Vagrant, its installation, configuration, advanced features, provisioning techniques, and automation capabilities for efficient virtual machine management.

Course Curriculum

- Lesson 1: Setting up Vagrant with AWS
- Lesson 2: Multi-machine Environment with Vagrant
- Lesson 3: Vagrant and AWS RDS Integration

- Lesson 4: Implementing Vagrant Provisioning Scripts
- Lesson 5: Vagrant and AWS Elastic Load Balancing (ELB)
- Lesson 6: Vagrant Teardown and Snapshots
- Lesson 7: Vagrant and AWS S3 Storage
- Lesson 8: Vagrant Networking with AWS
- Lesson 9: Scalable Vagrant with AWS Auto Scaling Groups
- Lesson 10: Vagrant Boxes and AWS AMI

Unit 22: Ansible I

This course is designed to provide comprehensive knowledge and hands-on experience in using Ansible for managing AWS infrastructure and automating various DevOps tasks. Through a series of practical tasks and documentation, learners will gain valuable insights into setting up Ansible on AWS EC2, utilising Ansible Ad-Hoc commands, writing basic Ansible Playbooks, managing AWS infrastructure with Ansible, understanding Ansible Roles and Galaxy, implementing dynamic inventory with AWS EC2, securing secrets using Ansible Vault, enabling Continuous Deployment with Ansible and AWS CodePipeline, integrating Ansible with AWS Lambda, and setting up monitoring for AWS resources managed by Ansible.

Key Learning Objectives

Upon successful completion of this course, learners will attain proficiency in the following key areas:

- Setting up Ansible on AWS EC2: Learn to launch an EC2 instance, establish SSH connections, and install Ansible while gaining insights into its benefits for configuration management in DevOps.
- Ansible Ad-Hoc Commands: Understand the utility of Ansible's Ad-Hoc commands and how to set up an inventory file with multiple EC2 instances to perform tasks like service management and user creation.
- Writing Basic Ansible Playbooks: Create Ansible Playbooks to install web servers like Nginx or Apache and execute them against EC2 instances, covering the anatomy of an Ansible playbook and working with Ansible modules.
- Managing AWS Infrastructure with Ansible: Develop Ansible Playbooks to create EC2 instances, set up an Elastic Load Balancer (ELB), and configure RDS instances, exploring Ansible AWS modules and Infrastructure as Code (IaC) principles.
- Ansible Roles and Galaxy: Create Ansible Roles for various tasks and leverage Ansible Galaxy Roles for setting up infrastructure components, gaining an understanding of Ansible Roles and the use of community roles.
- Dynamic Inventory with AWS EC2: Set up Ansible to use dynamic inventory based on AWS EC2 instances and execute playbooks using this dynamic inventory, highlighting the advantages of dynamic inventory and its integration with AWS EC2.
- Ansible Vault for Secure Secrets Management: Encrypt sensitive data using Ansible Vault and use it securely within playbooks, emphasising the importance of secrets management and how to work with Ansible Vault.

- Continuous Deployment with Ansible and AWS CodePipeline: Establish a CodePipeline to fetch code from a repository and deploy it to EC2 instances using Ansible Playbooks, integrating Ansible into AWS CI/CD workflows and understanding Continuous Deployment principles.
- Ansible and AWS Lambda Integration: Create AWS Lambda functions and invoke them using Ansible Playbooks, with an overview of AWS Lambda and its integration with Ansible.
- Setup Monitoring for AWS Resources Managed by Ansible: Configure EC2 instances managed by Ansible to send metrics to CloudWatch and set up CloudWatch alarms, highlighting the benefits of monitoring in DevOps and the integration of Ansible with Amazon CloudWatch.

Course Curriculum

- Lesson 1: Setting up Ansible on AWS EC2
- Lesson 2: Ansible Ad-Hoc Commands
- Lesson 3: Writing Basic Ansible Playbooks
- Lesson 4: Managing AWS Infrastructure with Ansible
- Lesson 5: Ansible Roles and Galaxy
- Lesson 6: Dynamic Inventory with AWS EC2
- Lesson 7: Ansible Vault for Secure Secrets Management
- Lesson 8: Continuous Deployment with Ansible and AWS CodePipeline
- Lesson 9: Ansible and AWS Lambda Integration
- Lesson 10: Setup monitoring for AWS resources managed by Ansible

Unit 23:Kubernetes Application Developer I

In this course, we delve into advanced topics, offering an in-depth exploration of setting up Amazon EKS (Elastic Kubernetes Service) and other critical aspects of DevSysOps Engineering. Through hands-on tasks and comprehensive documentation, learners will gain practical insights into various components.

Key Learning Objectives

Upon successful completion of this course, learners will attain proficiency in the following key areas:

- Introduction to Amazon EKS: Familiarise students with Amazon EKS and its advantages within the Kubernetes ecosystem.
- Persistent Storage Options: Explore various persistent storage options for Kubernetes when operating within AWS.
- Scaling Dynamics: Gain insights into the scaling dynamics specific to Kubernetes deployments on AWS.
- Networking Nuances: Delve into the intricate networking aspects and nuances within Amazon EKS.
- CI/CD Lifecycle with Kubernetes on AWS: Experience the complete CI/CD lifecycle while working with Kubernetes on AWS.

- **Microservice Connectivity:** Enhance microservice connectivity and communication within the Amazon EKS environment.
- **Monitoring Tools for EKS:** Equip students with essential monitoring tools tailored for Amazon EKS deployments.
- **Multi-Cluster Deployments:** Facilitate deployments across multiple Kubernetes clusters, emphasising versatility and scalability.
- **Application Security on EKS:** Strengthen security measures for applications running on Amazon EKS.
- **Application Migration Strategies:** Understand and employ effective strategies for migrating applications to Amazon EKS.
- **Kubernetes Application Developer Essentials:** Gain a foundational understanding of Kubernetes Application Development, Explore Kubernetes container orchestration and architecture, Master cluster creation using Minikube, Kubeadm, and Kind tools, Grasp YAML basics for Kubernetes configuration, Apply core Kubernetes Application Developer concepts through hands-on exercises.

Course Curriculum

- Lesson 1: Setting up Amazon EKS (Elastic Kubernetes Service)
- Lesson 2: Stateful Applications using EBS-backed Storage
- Lesson 3: Implementing Auto-scaling with AWS Metrics
- Lesson 4: Network Policies with Amazon VPC CNI
- Lesson 5: CI/CD with EKS using AWS CodeSuite
- Lesson 6: Service Discovery and Load Balancing with AWS App Mesh
- Lesson 7: Advanced Monitoring with AWS CloudWatch and Prometheus
- Lesson 8: Enhancing Security with AWS Secrets Manager and Kubernetes RBAC
- Lesson 9: Multi-cluster Deployments using Amazon EKS Anywhere
- Lesson 10: Migration of Applications to EKS

Unit 24: Kubernetes and Cloud Native Associates I

This course provides an in-depth exploration of Elastic Kubernetes Service (EKS) and its integration with Amazon Web Services (AWS). It equips learners with advanced knowledge and practical skills to effectively utilise EKS within cloud-native environments.

Key Learning Objectives

Upon successful completion of this course, learners will achieve proficiency in the following key areas:

- **Setting Up EKS (Elastic Kubernetes Service):** learners will master the process of setting up and configuring EKS, including cluster deployment and management.

- Implementing Persistent Storage with EKS using EFS: Learn to implement persistent storage solutions with EKS, utilising the Elastic File System (EFS) for data storage and management.
- Autoscaling in EKS: Gain expertise in auto scaling techniques within EKS to ensure optimal resource utilisation based on workload demands.
- EKS Networking with VPC and Load Balancers: Explore EKS networking capabilities, including Virtual Private Cloud (VPC) integration and load balancer configuration.
- CI/CD Pipeline Integration with EKS using AWS CodePipeline: Learn to integrate continuous integration and continuous delivery (CI/CD) pipelines with EKS through AWS CodePipeline.
- Implementing Helm Package Management in EKS: Master the deployment of Helm charts and package management in EKS, streamlining application installations.
- Implementing Service Mesh with AWS App Mesh and EKS: Understand how to implement service meshes using AWS App Mesh and EKS for enhanced microservices communication.
- Advanced Monitoring with Amazon CloudWatch and EKS: Explore advanced monitoring techniques by leveraging Amazon CloudWatch to gain insights into EKS clusters.
- Securing EKS Applications with AWS Secrets Manager: Enhance the security of EKS applications by utilising AWS Secrets Manager for sensitive data management.
- Implementing Canary Deployments in EKS: Learn to implement canary deployments in EKS, allowing for controlled testing of new features and updates.
- Demonstrating Understanding of Key Concepts: Demonstrate understanding of Kubernetes fundamentals, Show comprehension of container orchestration principles, Exhibit knowledge of cloud-native architecture concepts, Demonstrate understanding of cloud-native observability, Show comprehension of cloud-native application delivery principles.

Course Curriculum

Lesson 1: Implementing Canary Deployments in EKS

Lesson 2: Assessing Kubernetes Fundamentals and Cloud-Native Concepts

Lesson 3: Introduction to Elastic Kubernetes Service (EKS) and AWS Integration

Lesson 4: Setting Up and Configuring EKS Clusters

Lesson 5: Implementing Persistent Storage with EFS in EKS

Lesson 6: Autoscaling Strategies in EKS

Lesson 7: EKS Networking and Load Balancing in a Virtual Private Cloud (VPC)

Lesson 8: CI/CD Pipeline Integration with EKS using AWS CodePipeline

Lesson 9: Helm Package Management in EKS Deployments

Lesson 10: Service Mesh Implementation with AWS App Mesh and EKS

Lesson 11: Advanced Monitoring with Amazon CloudWatch in EKS

Lesson 12: Securing EKS Applications with AWS Secrets Manager

Unit 24: Kubernetes Administrator I

In this course, we delve into advanced topics related to Kubernetes and Amazon Web Services (AWS), focusing on optimising cloud-based container orchestration with Amazon Elastic Kubernetes Service (EKS). Through hands-on labs and comprehensive instruction, learners will gain a deep understanding of deploying multi-region EKS clusters, implementing cost-effective EKS spot instances, advanced VPC peering, Kubernetes Custom Resource Definitions (CRDs), advanced EKS logging using Fluentd and AWS Elasticsearch, GitOps workflows with ArgoCD, AWS Lambda integration for event-driven architectures, Service Mesh deployment with AWS App Mesh, advanced security using AWS GuardDuty and AWS WAF, and EKS backup and recovery with AWS Backup. Additionally, learners will grasp core concepts relevant to Certified Kubernetes Administrator (CKA), Kubernetes scheduling, logging, monitoring, cluster maintenance, security, storage, cluster design and installation, troubleshooting, and proficiency in JSON Path and Kubectl commands.

Key Learning Objectives

Upon successful completion of this course, learners will achieve expertise in the following key areas:

- Deploying Multi-Region EKS Clusters: Mastery of the deployment of EKS clusters across multiple regions.
- EKS Spot Instances and Cost Optimization: Proficiency in optimising EKS costs through the effective use of spot instances.
- Advanced VPC Peering with EKS: In-depth understanding and implementation of advanced VPC peering with EKS.
- Kubernetes Custom Resource Definitions (CRDs) in EKS: Comprehensive knowledge of using CRDs in EKS.
- Advanced EKS Logging with Fluentd and AWS Elasticsearch: Proficiency in advanced EKS logging with Fluentd and AWS Elasticsearch.
- Implementing GitOps Workflow in EKS with ArgoCD: Expertise in implementing GitOps workflows in EKS using ArgoCD.
- EKS and AWS Lambda Integration for Event-Driven Architectures: Proficiency in integrating EKS with AWS Lambda for event-driven architectures.
- Implementing Service Mesh with AWS App Mesh in EKS: Mastery of implementing service mesh using AWS App Mesh in EKS.
- Advanced Security in EKS using AWS GuardDuty and AWS WAF: Comprehensive understanding and implementation of advanced security measures in EKS using AWS GuardDuty and AWS WAF.
- EKS Backup and Recovery with AWS Backup: Proficiency in EKS backup and recovery using AWS Backup.
- Certified Kubernetes Administrator Core Concepts: A solid grasp of core CKA concepts.
- Kubernetes Scheduling: Understanding how Kubernetes scheduling works.
- Logging and Monitoring in Kubernetes: Proficiency in logging and monitoring within Kubernetes.
- Cluster Maintenance: Conceptualization of cluster maintenance in Kubernetes.
- Security in Kubernetes: A comprehensive understanding of security within Kubernetes.

- Storage in Kubernetes: Proficiency in handling storage in Kubernetes.
- Design & Install Kubernetes Cluster: Expertise in designing and installing Kubernetes clusters.
- Troubleshooting Kubernetes Failures: Proficiency in troubleshooting various types of Kubernetes failures.
- JSON Path and Kubectl Commands: Mastery of JSON Path and Kubectl commands for Kubernetes operations.

Course Curriculum

- Lesson 1: Deploying Multi-Region EKS Clusters
- Lesson 2: EKS Spot Instances and Cost Optimization
- Lesson 3: Advanced VPC Peering with EKS
- Lesson 4: Kubernetes Custom Resource Definitions (CRDs) in EKS
- Lesson 5: Advanced EKS Logging with Fluentd and AWS Elasticsearch
- Lesson 6: Implementing GitOps Workflow in EKS with ArgoCD
- Lesson 7: EKS and AWS Lambda Integration for Event-Driven Architectures
- Lesson 8: Implementing Service Mesh with AWS App Mesh in EKS
- Lesson 9: Advanced Security in EKS using AWS GuardDuty and AWS WAF
- Lesson 10: EKS Backup and Recovery with AWS Backup

Unit 26: Kubernetes Security Specialist I

This course delves into advanced topics in cloud security and Kubernetes management. Learners will engage in hands-on labs to gain practical expertise in securing Elastic Kubernetes Service (EKS) clusters, enhancing network policies with Calico, managing AWS secrets within Kubernetes, implementing pod security policies, configuring AWS Container Network Interface (CNI), monitoring Kubernetes audit logs with AWS CloudWatch, establishing authentication and authorization with OIDC, securing container images with ECR and Clair, and implementing Kubernetes service mesh with AWS App Mesh. Additionally, compliance monitoring with kube-bench and an exploration of cloud-native security principles will be covered.

Key Learning Objectives

Upon successful completion of this course, learners will acquire proficiency in the following key areas:

- Setting up a Secure EKS (Elastic Kubernetes Service) Cluster: learners will configure IAM roles for EKS, set up a secure VPC with security groups, launch and test EKS, and understand the significance of IAM roles, VPCs, and security groups in AWS.
- Network Policies with Calico: learners will install Calico on EKS, define and apply basic network policies, and validate their effectiveness while comprehending how network policies enhance security within Kubernetes.
- AWS Secrets with Kubernetes: learners will create AWS secret keys, store them as Kubernetes secrets, and access secrets within pods, all while understanding the Kubernetes secrets mechanism and its importance.

- Pod Security Policies: learners will set up default and custom Pod Security Policies (PSPs), test them with various pod configurations, and grasp how PSPs provide a security layer for pod execution.
- Configuring AWS CNI (Container Network Interface) for EKS: learners will set up EKS with a custom VPC, configure custom networking using AWS CNI, and validate their configurations, gaining insight into the significance of AWS CNI in EKS.
- Kubernetes Audit Logs with AWS CloudWatch: learners will establish audit logging in EKS, integrate it with CloudWatch, and learn to analyse and monitor logs while recognizing the importance of monitoring and auditing in Kubernetes security.
- Authentication and Authorization with OIDC: learners will set up an OIDC identity provider, integrate it with EKS, test access and Role-Based Access Control (RBAC), and gain knowledge about OIDC and RBAC mechanisms in Kubernetes.
- Container Images with ECR and Clair: learners will push images to Amazon Elastic Container Registry (ECR), integrate Clair with ECR, scan and analyse results, and understand the importance of scanning images for vulnerabilities.
- Implementing Kubernetes Service Mesh with AWS App Mesh: learners will set up App Mesh components, integrate them with existing EKS workloads, and manage traffic flow, comprehending the concept of a service mesh and its significance in microservices security.
- Compliance Monitoring with kube-bench: learners will install and configure kube-bench, run compliance checks, and interpret results while delving into the CIS benchmarks for Kubernetes and the importance of compliance.

Course Curriculum

- Lesson 1: Setting up a Secure EKS (Elastic Kubernetes Service) Cluster
- Lesson 2: Network Policies with Calico
- Lesson 3: AWS Secrets with Kubernetes
- Lesson 4: Pod Security Policies
- Lesson 5: Configuring AWS CNI (Container Network Interface) for EKS
- Lesson 6: Kubernetes Audit Logs with AWS CloudWatch
- Lesson 7: Authentication and Authorization with OIDC
- Lesson 8: Secure Container Images with ECR and Clair
- Lesson 9: Implementing Kubernetes Service Mesh with AWS App Mesh
- Lesson 10: Compliance Monitoring with kube-bench

Unit 27: AWS Solution Architecture I

Introduction:

This course is designed to provide students with a comprehensive understanding of Amazon Web Services (AWS) and equip them with the skills necessary to design, deploy, and manage effective, secure, and cost-efficient infrastructures on the AWS cloud platform. Throughout this course, students will engage in hands-on activities, gaining practical experience in various aspects of AWS solution architecture.

Key Learning Objectives:

- Gain a foundational understanding of AWS and the tools necessary for environment setup.
- Develop proficiency in deploying a CI/CD pipeline using AWS DevOps tools.
- Acquire knowledge of monitoring, management, and auditing tools on AWS.
- Develop expertise in deploying and managing highly available and scalable applications using Amazon EC2.
- Gain proficiency in working with AWS storage services for data storage, backup, and retrieval.
- Establish a secure AWS environment through best practices in networking and security.
- Develop an in-depth understanding of AWS security and user management.
- Explore managed relational database services on AWS.
- Gain insights into GRC (Governance, Risk, and Compliance) aspects within AWS and centralised management.
- Integrate knowledge from previous labs to design a secure and scalable AWS infrastructure.

Course Curriculum:

- Lesson 1: AWS Essentials & Environment Setup
- Lesson 2: Deploying DevOps on AWS
- Lesson 3: SysOps Monitoring & Management
- Lesson 4: High Availability & Elasticity with EC2
- Lesson 5: AWS Storage Solutions and Management
- Lesson 6: Secure Architecture Design
- Lesson 7: AWS Identity and Access Management (IAM)
- Lesson 8: AWS RDS & Database Management
- Lesson 9: Governance, Risk, and Compliance (GRC) on AWS
- Lesson 10: Capstone Project - Comprehensive AWS Solution Design

Unit 28: Microsoft Azure Administrator I

Introduction

Welcome to the course on "Microsoft Azure Administration Essentials." In this course, we will provide you with a comprehensive understanding of the foundational principles, methodologies, and best practices required for effective administration within the Microsoft Azure platform.

Key Objectives

Throughout this course, we aim to achieve the following key objectives:

- **Azure Environment Familiarity:** We will immerse you in the Microsoft Azure ecosystem, ensuring that you become familiar with essential components such as the Azure Portal, Azure CLI, PowerShell, and foundational Azure services.

- Resource Management and Deployment: You will acquire the skills needed to deploy, manage, and monitor Azure resources, with a focus on Resource Groups, ARM templates, and Azure Policy.
- Virtual Networking Essentials: We will delve into the concepts of Azure virtual networks, subnets, and related networking tools, promoting best practices for secure and efficient cloud connectivity.
- Azure Identity and Access Management: You'll gain a comprehensive understanding of Azure Active Directory, emphasising user governance, authentication mechanisms, and role-based access controls.
- Storage and Data Management: We will educate you on the functionalities and advantages of Azure storage solutions, including Azure Blob Storage, Azure Disk Storage, and Azure File Shares.
- Operational Insights: We'll introduce tools like Azure Monitor and Azure Security Center, enabling you to glean actionable insights from cloud metrics and adopt robust security postures.
- Continuity and Recovery: You'll be equipped with strategies and tools like Azure Backup and Azure Site Recovery, ensuring data integrity and availability in diverse scenarios.
- Cost Management and Optimization: We will foster an understanding of Azure cost structures, equipping you with the tools and practices to manage and optimise your cloud expenditure effectively.

By the conclusion of this course, you will possess both the theoretical knowledge and practical experience necessary to navigate the complexities of the Microsoft Azure environment, embodying the roles of efficient and resourceful Azure administrators.

Course Curriculum:

- Lesson 1: Azure Fundamentals & Environment Setup
- Lesson 2: Infrastructure as Code with Azure Resource Manager (ARM)
- Lesson 3: Azure Networking & Security Basics
- Lesson 4: Azure Active Directory & Identity Management
- Lesson 5: Azure Storage Solutions for DevOps
- Lesson 6: Monitoring & Operations with Azure Monitor and Log Analytics
- Lesson 7: Azure Security Center for Cloud Security
- Lesson 8: Azure Policy & Blueprints for GRC
- Lesson 9: Azure DevTest Labs for DevOps & SysOps
- Lesson 10: Capstone Project - Holistic Azure Solution Design

Unit 29: Professional Cloud Security I

Introduction

This course aims to provide students with a comprehensive understanding and proficiency in the field of cloud cybersecurity. Focusing on essential aspects such as DevOps, SysOps, cloud security, traditional cybersecurity, and Governance, Risk, and Compliance (GRC), the curriculum is designed to shape students into skilled cloud security professionals. Through a combination of

theoretical concepts and practical experience, students will be well-prepared to tackle contemporary cybersecurity challenges in cloud environments.

Key Objectives:

- **Foundational Cloud Security:** To furnish students with a solid foundation in core principles, methodologies, and challenges of cloud security across various cloud platforms.
- **DevOps & SysOps in Cloud Security:** To explore the integration of security into operations, emphasising how security principles are embedded within DevOps (SecDevOps) and SysOps.
- **Advanced Cloud Cybersecurity Techniques:** Delve into advanced security mechanisms, architectures, and technologies crucial for safeguarding cloud-based assets and infrastructures.
- **Governance, Risk, and Compliance (GRC):** To cultivate a robust understanding of GRC within the context of cloud environments, ensuring students are skilled at navigating regulatory landscapes and implementing compliant security measures.
- **Practical Cybersecurity in Cloud:** Hands-on experiences with popular cloud platforms, simulating real-world scenarios, threats, and security implementations.
- **Collaboration & Cross-functional Engagement:** Promote collaboration among development, system engineering, and operational teams, fostering a holistic approach to security and compliance in the cloud.

Upon completion of this course, students will be well-prepared to lead cloud security initiatives, comprehend and mitigate potential cybersecurity threats, and create secure, compliant, and efficient cloud environments.

Course Curriculum:

- Lesson 1: Cloud Security Essentials & Environment Setup
- Lesson 2: Infrastructure as Code & Security Automation
- Lesson 3: Network Security & Micro-segmentation in Cloud
- Lesson 4: Identity & Access Management (IAM)
- Lesson 5: SecDevOps Integration & Continuous Security Monitoring
- Lesson 6: Data Security & Encryption Practices in Cloud
- Lesson 7: Cloud Security Posture Management & Compliance Scanning
- Lesson 8: Incident Response & Forensics in Cloud Environments
- Lesson 9: Advanced Threat Protection & Cloud-native Security Solutions
- Lesson 10: GRC in Action: Audit, Remediate & Report

Unit 30: Cloud Security Standards Review I

Introduction

This unit is designed to equip learners with an in-depth understanding of cloud security, exploring both foundational concepts and practical applications in a cloud environment. Learners will delve into the intricacies of cloud architecture, data security, application security, and the necessary

operations to ensure robust cloud security. The unit emphasises the integration of theory and practice, enabling learners to make informed decisions related to cloud security in real-world scenarios.

Key Learning Objectives:

Upon successful completion of this unit, learners will be able to:

-
- Recognize the significance of CCSK as a standard in cloud security and identify its primary themes and areas of knowledge.
- Navigate and effectively utilise the learning environment and understand the significance and application of various learning tools and resources.
- Summarise foundational principles guiding cloud security and distinguish between different security models in a cloud environment.
- Describe key components of cloud architecture and evaluate security implications associated with different cloud architectures.
- Identify key threats and vulnerabilities at the infrastructure level of cloud computing and implement strategies for securing cloud infrastructure.
- Develop a comprehensive cloud security risk management plan and apply principles of risk assessment, mitigation, and monitoring in a cloud environment.
- Understand data protection requirements and methodologies in the cloud and implement encryption, access controls, and other security measures for data security.
- Evaluate the security aspects of cloud-based applications and implement appropriate user authentication, authorization, and other security measures.
- Understand the lifecycle of cloud security operations, from planning to monitoring, and employ best practices in incident response, monitoring, and auditing within a cloud environment.

Course Curriculum:

- Lesson 1: Introduction to Cloud with Terraform (DevOps)
 - Lesson 2: Hardening Cloud Infrastructure using Ansible (SysOps)
 - Lesson 3: Intrusion Detection with Wazuh (Cyber Security)
 - Lesson 4: Cloud Data Encryption using Vault (Cloud Security)
 - Lesson 5: Continuous Compliance Checking with Open Policy Agent (GRC)
 - Lesson 6: Serverless Security with OWASP ZAP (DevOps & Cloud Security)
 - Lesson 7: Monitoring Cloud Traffic with ELK Stack (SysOps)
 - Lesson 8: Application Security Scanning with OWASP Dependency-Check (DevOps & Cyber Security)
 - Lesson 9: Container Security with Clair (SysOps & Cloud Security)
 - Lesson 10: GRC Policy Enforcement with Kyverno (GRC & Cloud Security)
-

Unit 31: ISSAP Architecture Professional Review I

The purpose of this course is to provide a comprehensive understanding of the advanced facets within the Information Systems Security Architecture field. Grounded in the framework set forth by the International Information System Security Certification Consortium (ISC²), this course centres on the six domains of the Information Systems Security Architecture Professional (ISSAP) concentration. It aims to equip participants with the expertise required to formulate, create, and oversee a security architecture that aligns with an organisation's goals and adheres to regulatory standards.

Key Learning Objectives:

Upon successful completion of this unit, learners will be able to:

- Gain a comprehensive understanding of the process involved in establishing and configuring an Identity and Access Management (IAM) system.
- Demonstrate the capability to monitor real-time security events and visualise patterns using the ELK Stack.
- Create Ansible playbooks to automate the process of hardening infrastructure security in accordance with CIS Benchmarks.
- Ensure that infrastructural components adhere to established compliance policies by employing policy-as-code with OPA.
- Formulate a threat model for a sample application, prioritise identified threats, and propose mitigation strategies.
- Safeguard a web application against common security threats utilising ModSecurity and OWASP CRS.
- Deploy a secure Kubernetes cluster and acquire an understanding of its security configurations.
- Analyse the codebase to identify security vulnerabilities and assess code quality through the use of SonarQube.
- Comprehend the principles governing data encryption and decryption, employing OpenSSL as a tool.
- Implement a Zero Trust security model by leveraging WireGuard VPN technology.

Course Curriculum

- Lesson 1: Identity Management with Keycloak
- Lesson 2: Security Monitoring with ELK Stack
- Lesson 3: Hardening Infrastructure with Ansible
- Lesson 4: Compliance Auditing with Open Policy Agent (OPA)
- Lesson 5: Threat Modelling with OWASP Threat Dragon
- Lesson 6: Web Application Firewall (WAF) with ModSecurity
- Lesson 7: Secure Container Orchestration with Kubernetes
- Lesson 8: Secure Code Analysis with SonarQube
- Lesson 9: Data Encryption with OpenSSL
- Lesson 10: Zero Trust Architecture with WireGuard VPN

Unit 32: Cloud Assurance: Zero Trust Frameworks

In this course, we delve into the fundamentals of Zero Trust Architecture and Software-Defined Perimeter, providing essential knowledge for professionals.

Key Learning Objectives

Upon successful completion of this course, learners will attain proficiency in the following key areas:

- Zero Trust Architecture Essentials: Gain a comprehensive understanding of the principles and foundations of Zero Trust Architecture, emphasising trust-based security models.
- Software-Defined Perimeter Intro: Explore the introductory concepts of Software-Defined Perimeter, highlighting its significance in modern security paradigms.
- SDP: Features and Technological Insights: Dive deeper into Software-Defined Perimeter, examining its features and technological insights, and how they contribute to enhanced security.
- Software-Defined Perimeter Architecture Deep Dive: Take an in-depth look into the architecture of Software-Defined Perimeter, uncovering its components and how they work together.
- Zero Trust Strategic Planning: Learn how to strategically plan for implementing Zero Trust principles within your organisation's security framework.
- Zero Trust Deployment Blueprint: Develop a blueprint for deploying Zero Trust Architecture and Software-Defined Perimeter effectively.

Course Curriculum

- Lesson 1: Zero Trust Architecture Essentials
- Lesson 2: Software-Defined Perimeter Intro
- Lesson 3: SDP: Features and Technological Insights
- Lesson 4: Software-Defined Perimeter Architecture Deep Dive
- Lesson 5: Zero Trust Strategic Planning
- Lesson 6: Zero Trust Deployment Blueprint

Unit 33: LinkedIn Course for Job Seekers

Unit Objectives:

- Enable learners to effectively use LinkedIn for job searching and freelancing opportunities
- Develop skills in personal branding and content marketing on LinkedIn
- Build professional networks and identify hidden job markets
- Create an optimized LinkedIn profile that attracts recruiters and clients

Unit Curriculum:

- Understanding LinkedIn's ecosystem for job search and freelancing
- Branding as a subject matter expert and thought leader

- Content and keyword targeting strategies
- About Summary optimization and content relevance
- Networking and identifying the hidden job market
- LinkedIn Marketplace for freelancers
- Tools for targeting global emerging technology opportunities
- Q&A live sessions with LinkedIn coach
- Toolkits, worksheets, and best practice guides

Unit 34: IELTS Academic and General Training

Unit Objectives:

- Prepare students for the IELTS examination
- Improve reading, writing, listening, and speaking skills
- Develop strategies for attempting each section of the IELTS test
- Build confidence in English language usage for academic and general contexts

Unit Curriculum:

- Reading for gist, scanning details, and in-depth reading
- Listening for gist, important details, and deeper meanings
- Writing cohesive essays (argumentative, descriptive, discursive)
- Letter writing and academic analysis of graphs, charts, and tables
- Speaking fluently in work-based and academic scenarios
- Everyday conversation skills in English
- Test-taking strategies and exam techniques

COPYRIGHT NOTICE

This document, including all content, text, images, graphics, logos, and course materials, is the exclusive property of ALNAFI E-LEARNING (PRIVATE) LIMITED.

Unauthorized Use Prohibited

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of the College.

Permitted Use

This document is provided for informational and educational purposes only. You may view, download, and print this document for personal, non-commercial use, provided that:

- All copyright and proprietary notices are retained.
- The content is not modified or altered in any way.

Where Can I find more information?

UK Office Address:

167-169 Great Portland Street 5th Floor London W1W 5PF

Regional Office:

Pakistan: D-182, Block-7, Gulshan-e-Iqbal, Karachi, Sindh, Pakistan.

Contact Us:

+92-304-1110 400, +1 (647) 680-0258 (WhatsApp)

Send Us Message Support@alnafi.com

Visit: **www.alnafi.com**

