

Diploma in Artificial Intelligence Operations

EduQual Level 6 Endorsed Diploma

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

Version: 1.0

© 2026 Al Nafi E-Learning Private Limited. All rights reserved.

Table of Contents

1. About the Diploma	5
2. Key Features of the Diploma	6
3. About the Diploma Program Endorsed by EduQual	6
4. How the Programme Works	7
5. About Al Nafi International College	7
6. Program Eligibility Criteria and Application Process	7
6.1. Eligibility Criteria	8
6.2. Application Process	8
7. Connect with the Support Operations Center	8
8. Program Outcomes	9
9. Who Should Enrol in this Program?	10
10. Learning Path	12
11. Assessment Information	13
11.1. Assessment Overview	13
Assessment Components	13
11.2. Al Razzaq Lab Assignments (70% weightage in overall Grade)	14
What Are They?	14
How Are They Graded?	14
What If You Need to Resubmit?	14
11.3. Multiple Choice Questions (15% of Your Grade)	15
Assessment Format	15
Attempts and Scoring	15
Diploma Program Access Period	15
11.4. English Language Exam (15% of Your Grade)	16
Mandatory Requirement	16
Submission Requirements	16
Verification and Compliance	16
Why Is This Required?	16
11.5. Al Razzaq Labs Program Access	16
Prerequisites for Lab Access	16
Lab Components	17
Additional Features and Support	17
11.6. Grading Criteria	18
Grade Boundaries	18
Example Calculation	
For a student:	18
Example: Overall Grade Calculation	19
Quick Reference Table	20
11.7. Academic Integrity	20
Violation Response	21
11.8. Support for Students	21
11.9. Accessibility and Reasonable Adjustments	21

11.10. Appeals Process	22
Complete Course Units (61 Units)	22
Unit 1: Linux Deep Dive	22
Unit 2: Python Deep Dive	23
Unit 3: Certified Information Systems Security Professional (CISSP)	23
Unit 4: Red Hat Enterprise Linux (RHEL)	24
Unit 5: AWS Solutions Architect	24
Unit 6: Python Automation	25
Unit 7: Certified Kubernetes Application Developer (CKAD)	26
Unit 8: Certified Kubernetes Administrator (CKA)	26
Unit 9: Ansible Deep Dive	27
Unit 10: DevOps Docker Deep Dive	28
Unit 11: Certificate of Cloud Security Knowledge (CCSK)	28
Unit 12: Certified Kubernetes Security Specialist (CKS)	29
Unit 13: Python Flask	30
Unit 14: Python Selenium	31
Unit 15: Docker Deep Dive I	31
Unit 16: Bash Script Deep Dive I	32
Unit 17: Python Automation Deep Dive I	33
Unit 18: Python Selenium I	34
Unit 19: JIRA with Python I	35
Unit 20: Python Flask I	36
Unit 21: Vagrant I	37
Unit 22: Ansible I	38
Unit 23:Kubernetes Application Developer I	40
Unit 24: Kubernetes and Cloud Native Associates I	41
Unit 25: Kubernetes Administrator I	42
Unit 26: Kubernetes Security Specialist I	44
Unit 27: AWS Solution Architecture I	45
Unit 28: Microsoft Azure Administrator I	46
Unit 29: Professional Cloud Security I	47
Unit 30: Cloud Security Standards Review I	48
Unit 31: ISSAP Architecture Professional Review I	49
Unit 32: Cloud Assurance: Zero Trust Frameworks	50
Unit 33: Docker Deep Dive II	51
Unit 34: Bash Script Deep Dive II	52
Unit 35: Python Automation Deep Dive II	53
Unit 36: Python Selenium II	54
Unit 37: JIRA with Python II	55
Unit 38: Python Flask II	56
Unit 39: Vagrant II	57
Unit 40: Ansible II	58
Unit 41:Kubernetes Application Developer II	59
Unit 42: Kubernetes and Cloud Native Associates II	60

Unit 43: Kubernetes Administrator II	61
Unit 44: Kubernetes Security Specialist II	62
Unit 45: AWS Solution Architecture II	63
Unit 46: Microsoft Azure Administrator II	64
Unit 47: Professional Cloud Security II	65
Unit 48: Cloud Security Standards Review II	66
Unit 49: ISSAP Architecture Professional Review II	67
Unit 50: Artificial Intelligence II	68
Unit 51: Python Programming for Machine Learning II	68
Unit 52: Deep Learning II	69
Unit 53: Machine Learning - Mathematics and Python Implementation II	70
Unit 54: Advanced topics in Machine Learning II	71
Unit 55: Practical Applications of Machine Learning II	72
Unit 56: Deep Learning Open Source Perspective	73
Unit 57: Machine learning Model Development and Deployment II	74
Unit 58: Computer Vision II	75
Unit 59: Natural Language Processing II	76
Unit 60: LinkedIn Course for Job Seekers	77
Unit 61: IELTS Academic and General Training	77
COPYRIGHT NOTICE	78
Unauthorized Use Prohibited	78

1. About the Diploma

Embark on a thrilling technological voyage with our "Diploma in Artificial Intelligence Operations." This meticulously crafted program is your gateway to exciting careers in Artificial Intelligence, DevOps, SysOps, Cloud Engineering, and Cyber Security. Immerse yourself in an enriching curriculum that delves deep into the heart of these dynamic fields.

One distinguishing feature of this program is the hands-on learning experience it offers. Through our home grown AI 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.

Remarkably, this program seamlessly blends specific units from various diploma programs, empowering you to develop a comprehensive understanding of emerging technologies and enhance your employability with a diverse skill set.

At its core, this program is geared towards employability. We offer a wealth of open-source, vendor-neutral resources, instructional videos, hands-on exercises, cloud labs, and assignments. To enrich your practical learning experience, we provide step-by-step guidance and opportunities to engage with instructors through community discussions, forums, and live online classes.

In essence, the "Diploma in Artificial Intelligence Operations" at EduQual Level 6 is a comprehensive and hands-on journey, meticulously designed to prepare you for thriving careers in the dynamic fields of Artificial Intelligence, DevOps, SysOps, Cloud Engineering, and Cyber Security. Graduates of this program are primed to excel in the technology industry, thanks to hands-on experience and a curriculum finely tuned to meet the demands of the ever-evolving global job market, making them job-ready within 3 to 6 months.

Our mission is to offer an unmatched diploma program on a global scale, merging Generative AI, open-source methodologies, and AWS Cloud-native technologies. This program encompasses AI, DevOps, SysOps, Cyber Security, Cloud Cyber Security, Governance, Risk, and Compliance, enabling you to deeply engage in the interconnected worlds of DevOps, SysOps, and AI, especially in the cloud domain.

Our teaching philosophy places a strong emphasis on active learning, providing real-world applications with the support of AI Nafi Cloud's container labs, allowing you to put theoretical knowledge to the test. As the digital landscape evolves, so do its vulnerabilities. Our diploma incorporates comprehensive modules on cloud security, preparing you to design, implement, and assess robust security strategies for cloud infrastructures.

Our academic design aligns seamlessly with the Regulated Qualifications Framework (RQF) Level 6, fostering collaboration between development, system engineering, and operational divisions. Through the use of Cloud resources, we instil the finer points of workflow automation, creating an integrated, multifaceted workspace.

We offer a holistic educational journey, complete with an AI Razzaq program that leads to a professional portfolio. Supported by resume-building sessions and interview masterclasses, we aim to shape students who are industry-ready and self-assured.

Graduates from our program are poised to take on a spectrum of roles, including DevOps Engineer, SysOps Engineer, Cloud Engineer, Site Reliability Engineer (SRE), Infrastructure Engineer, Automation Engineer, and Quality Assurance Engineer. We envision our graduates as technical maestros and pioneering leaders in the ever-evolving landscapes of AI, DevOps, and SysOps. Join us on this transformative educational journey into the future of technology!

2. Key Features of the Diploma

- EduQual endorsement, a globally recognised qualification
- Nearly 2500 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
- Postgraduate 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

Our Level 6 Diploma in Artificial Intelligence Operations, endorsed by EduQual, is a gateway to thriving careers in Artificial Intelligence, Cyber Security, Cloud Computing, DevOps, and SysOps. EduQual, a globally recognized awarding organisation, bestows top-tier qualifications that enjoy widespread esteem from employers and academic institutions worldwide. Endorsed by EduQual, this diploma program signifies our unwavering commitment to maintaining the highest standards of education and equipping students with in-depth cloud computing expertise.

This diploma is the ideal choice for individuals aspiring to enhance their skills in Artificial Intelligence, SysOps, DevOps, and cloud computing, thus elevating their career prospects in this rapidly evolving sector. Furthermore, as it aligns with Level 6 of the Regulated Qualifications Framework (RQF), learners who earn the EduQual certificate may be eligible for full exemptions in an undergraduate program, propelling them further along the path of academic and professional success.

Upon completion of this diploma program, students will:

- Upon program completion, graduates receive two EduQual diploma certificates (Level 5 and Level 6) along with corresponding transcripts for each diploma level.
- Graduates are eligible for Al Nafi Alumni membership and may seek admission into Master's degree programs.
- Students who opt not to pursue further studies can directly apply for jobs based on the skills acquired during the program.

4. How the Programme Works

All students will study this Diploma via a structured pathway that seamlessly combines two qualifications. Upon enrolment, students gain immediate access to the student portal, which contains the integrated coursework for both the Diploma in DevSysOps Engineering (EduQual Level 5) and the Diploma in Artificial Intelligence Operations (EduQual Level 6), offering full visibility of the programme's scope from day one. However, academic progression is strictly sequential: students must successfully complete and pass all modules of the Level 5 Diploma before they are permitted to submit work for, or advance to, the Level 6 Diploma.

5. About Al Nafi International College

Al 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.

6. Program Eligibility Criteria and Application Process

To apply for the Diploma in Artificial Intelligence operations at EduQual Level 6, individuals who are interested will need to register for the diploma through the website. The provided link <https://alnafi.com/courses/diploma-in-artificial-intelligence-ops> 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.

6.1. 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:

All learners must possess the following:

- A laptop 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.

6.2. 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

7. 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.

8. Program Outcomes

- Critically evaluate containerisation architecture and its strategic role in modern deployment, formulating robust strategies for scalable, production-grade systems.
- Synthesise operational, systems, and AI principles within cloud contexts; critically deconstruct, optimise, and justify advanced scripting solutions to resolve complex, real-world operational challenges.
- Design and implement advanced automation frameworks, integrating diverse libraries and APIs, while critically appraising efficiency, maintainability, and scalability for complex operational and AI scenarios.
- Critically apply web-automation tools to automate intricate interactions; evaluate dynamic web structures and formulate resilient automation strategies for production-grade cloud environments.
- Construct and manage integrated project-management and scripting solutions, synthesising agile methodologies, advanced reporting, serverless computing, and cloud configurations to strategically optimise enterprise project management and operational automation.
- Design and implement lightweight web-application frameworks, critically evaluating cloud deployment architectures using platform-as-a-service, relational databases, serverless functions, and API gateways for scalable, secure delivery.
- Formulate and orchestrate cloud-native development workflows, critically appraising integrated development environments, container orchestration, and serverless computing to engineer reproducible, scalable, and portable environments.
- Synthesise advanced configuration automation with Infrastructure as Code leadership, evaluating its integration within operational toolchains and justifying architectural decisions for managing and scaling dynamic cloud infrastructures.
- Critically evaluate core container orchestration architectures and cloud integrations, designing strategic application-deployment models that align with operational and AI requirements.
- Design and justify deployment strategies for applications on managed Kubernetes services and open-source platforms, critically analysing high availability, fault tolerance, and comprehensive security postures.
- Formulate and manage cluster deployments in cloud-native environments, integrating them seamlessly into operational and AI workflows while evaluating performance, resilience, and ethical dimensions.
- Critically evaluate and harden containerised clusters in cloud-native ecosystems, implementing robust protective frameworks specifically tailored for managed cloud services and open-source technologies.
- Synthesise advanced cloud architectural principles, designing and justifying complex, integrated, and cost-optimised solutions within the broader context of operations and systems management.

- Design, deploy, and manage complex cloud solutions, critically evaluating operational challenges and formulating strategic mitigation approaches for identity, networking, storage, continuity, and cost governance.
- Critically analyse global cyber threats, formulate strategic security architectures, and justify robust, cross-platform protective measures across diverse cloud providers.
- Appraise and integrate professional auditing and governance principles into cloud assurance practices, formulating comprehensive strategies to lead and transform organisational security governance.
- Design and manage robust governance, compliance, and risk-management frameworks, critically evaluating their alignment with regulatory standards and strategic organisational objectives across multiple critical security domains.
- Formulate and justify artificial-intelligence strategies to enhance cloud security, optimise operational pipelines, and embed governance and compliance principles, while critically evaluating the ethical, societal, and operational implications of AI deployments.
- Synthesise advanced programming constructs with machine-learning and AI development, critically appraising their integration within operational, security, and compliance frameworks to tackle unpredictable real-world data challenges.
- Design, implement, and optimise deep-learning solutions, critically evaluating their integration with security controls and operational best practices for resilient deployment.
- Synthesise rigorous mathematical foundations with implementation skills, justifying secure, scalable integration into cloud environments and operational pipelines.
- Critically evaluate and implement cutting-edge machine-learning methodologies, justifying secure cloud deployment aligned with operational principles and open-source collaboration.
- Design and implement machine-learning solutions to detect, predict, and mitigate cyber threats, critically evaluating their empirical efficacy in securing and defending digital infrastructures.
- Formulate, implement, and benchmark state-of-the-art deep-learning algorithms, critically appraising their performance, trade-offs, and applicability in complex, resource-constrained environments.
- Design, refine, and justify end-to-end model-deployment pipelines for cybersecurity and cloud security, integrating open-source tools and evaluating real-world performance metrics.
- Design and tailor specialised algorithms, critically appraising their integration into cybersecurity, cloud security, and operational frameworks using open-source libraries to solve practical automation challenges.
- Formulate and implement natural-language-processing strategies to fortify cybersecurity monitoring and optimise cloud operations, critically evaluating their impact, limitations, and effectiveness in dynamic threat landscapes.

9. Who Should Enrol in this Program?

This Diploma in Artificial Intelligence Operations is designed for:

- School, College and university students looking to gain admissions in the Master'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:

- AI Engineer, DevOps Engineer, AI Solutions Architect
- Site Reliability Engineer (SRE), AI Project Manager, Machine Learning Engineer
- Cloud Security Engineer, Computer Vision Specialist, Natural Language Processing Specialist
- SysOps Engineer, 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
- 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

10. 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. Docker Deep Dive II
34. Bash Script Deep Dive II
35. Python Automation Deep Dive II
36. Python Selenium II
37. JIRA with Python II

38. Python Flask II
39. Vagrant II
40. Ansible II
41. Kubernetes Application Developer II
42. Kubernetes and Cloud Native Associate II
43. Kubernetes Administrator II
44. Kubernetes Security Specialist II
45. Kubernetes and Cloud Native Security Associate II
46. AWS Solution Architecture II
47. Microsoft Azure Administrator II
48. Professional Cloud Security II
49. Cloud Security Standards Review II
50. ISSAP Architecture Professional Review II
51. Artificial Intelligence II
52. Python Programming for Machine Learning II
53. Deep Learning II
54. Machine Learning - Mathematics and Python Implementation II
55. Advanced topics in Machine Learning II
56. Practical Applications of Machine Learning II
57. Deep Learning Open Source Perspective
58. Machine learning Model Development and Deployment II
59. Computer Vision II
60. Natural Language Processing II
61. LinkedIn Course for Job Seekers
62. IELTS Academic and General Training
63. Pass all MCQs and all AI Razzaq part 1 labs given for the diploma
64. Achieve a 6.5 band or more in IELTS for UKVI
65. Attain EduQual Certificate.

11. 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.

11.1. 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.

11.2. 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

11.3. 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.

11.4. 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 Al Nafi Student Portal or verified directly through official providers.

Verification and Compliance

Al 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 Al 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.

11.5. Al Razzaq Labs Program Access

Prerequisites for Lab Access

Access to Al 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

11.6. 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.

11.7. 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

11.8. 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

11.9. 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@alnaficoll.com

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

11.10. 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@alnaficoll.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 (61 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, WTFForms.

- 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 25: 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

Diploma in Artificial Intelligence Operations–Learner Handbook–v1

© 2026 Al Nafi E-Learning Private Limited. | <https://alnafi.com>

- 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

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

Unit 33: Docker Deep Dive II

The course "Docker Deep Dive II" 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. In this comprehensive unit, "Docker Deep Dive II," learners will embark on an extensive exploration of containerization technology, with a primary focus on Docker. Docker has revolutionised software deployment practices within the realms of DevOps, SysOps, and AI, making it an essential tool in modern IT operations. This course seeks to equip participants with a deep understanding of core containerization principles and Docker's pivotal role in contemporary software deployment. By diving into practical exercises and real-world scenarios, learners will gain hands-on technical proficiency in creating, deploying, and managing Docker containers. The course will also emphasise Docker's integration with DevOps and SysOps practices, fostering collaborative problem-solving and ethical considerations related to containerized applications. Upon completion, learners will be well-prepared to harness Docker's capabilities, seamlessly integrating containerized solutions into diverse operational contexts.

Key Learning Objectives

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

- Understand fundamental principles of DevOps and Docker architecture.
- Develop Docker files and containers, showcasing proficiency in advanced Docker file concepts and commands.
- Master Docker volume management, multi-stage compositions, and Docker Compose.
- Integrate Docker with cloud services (e.g., AWS), and manage Docker images in version control repositories (GitHub/GitLab).
- Analyse and configure advanced Docker networking, including inter-container linking and Docker Swarm.
- Implement Docker monitoring, secrets management, and advanced deployment techniques.

- Apply comprehensive integration skills using open-source and AWS cloud-native technologies.
- Understand the role and responsibilities of a DevOps Administrator.
- Highlight ethical considerations and responsibilities associated with deploying applications in containerized environments.

Course Curriculum

- Lesson 1: Installing Docker and Initial Commands
- Lesson 2: Crafting Docker Files and Containers
- Lesson 3: Docker Compose & Data Containers
- Lesson 4: Docker Image Path Manipulations and Networking Essentials
- Lesson 5: Docker Image Operations with GitHub and GitLab Repositories
- Lesson 6: Automating Docker Operations using AWS Cloud-Native Services
- Lesson 7: Creating and Managing Docker Networks
- Lesson 8: Working with Local Docker Repositories
- Lesson 9: Deploying Jboss Using Docker and Docker Alias Techniques
- Lesson 10: Comprehensive Integration using Open Source and AWS Cloud-Native Technologies

Unit 34: Bash Script Deep Dive II

In the dynamic intersection of DevOps, SysOps, and AI within the evolving landscape of cloud technologies, the course "Bash Script Deep Dive II" aims to provide learners with an in-depth understanding of these critical domains and their symbiotic relationship in the context of cloud technology. Through a series of comprehensive key learning objectives and hands-on lab experiences, this course equips students with the knowledge and skills required to navigate, innovate, and excel in this dynamic field. By the end of this unit, learners will possess a profound and critical understanding of DevOps, SysOps, and AI within the cloud context, empowering them to create real-world solutions.

Key Learning Objectives

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

- Gain a comprehensive grasp of DevOps, SysOps, and AI principles in the context of cloud technology.
- Develop the analytical skills to deconstruct and critically evaluate complex Bash scripts.
- Understand the role and interplay of variables, conditions, and advanced functionalities.
- Delve deeper into Bash scripting, covering loops, images, containers, networks, and volumes.
- Learn to design multifaceted scripts and employ conditional statements and pipelines with precision.
- Assess and optimise Bash script applications for efficiency, security, and scalability.
- Challenge students to develop sophisticated real-world solutions.

- Apply, evaluate, and adapt Bash scripting concepts in complex real-world scenarios through practical phases and advanced hands-on exercises.

Course Curriculum

- Lesson 1: Setting up and executing basic Bash operations on AWS CloudShell.
- Lesson 2: Implementing Conditional Decision Making using Bash on AWS EC2 instances.
- Lesson 3: Using Bash loops for AWS S3 batch operations.
- Lesson 4: Advanced script techniques with AWS Lambda function triggers.
- Lesson 5: Bash array operations integrated with AWS DynamoDB.
- Lesson 6: AWK Scripting in Bash for Data Processing in AWS Redshift.
- Lesson 7: Data Transformations with Bash and AWS Glue ETL jobs.
- Lesson 8: Implementing the Find command on AWS EFS for file operations.
- Lesson 9: Scheduling Bash scripts using AWS EventBridge and Lambda.
- Lesson 10: End-to-end automation scenario using Bash scripting in AWS environment.

Unit 35: Python Automation Deep Dive II

In the course "Python Automation Deep Dive II," learners will delve into the advanced aspects of Python automation within the context of DevOps, SysOps, and AI. This comprehensive program aims to equip students with the knowledge and skills necessary to master Python automation, enabling them to excel in real-world scenarios. The course focuses on key learning objectives and practical labs, ensuring that students not only gain theoretical knowledge but also practical experience in utilising Python for automation in various domains.

Key Learning Objectives

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

- Develop an advanced understanding of Python, including intricate topics such as data structures, data types, control mechanisms, and modular programming techniques.
- Gain the ability to create and execute Python scripts that automate complex tasks, such as cloud resource management, data analytics, and AI-driven operations.
- Proficiency in integrating various libraries and APIs to craft sophisticated automation solutions for real-world challenges.
- Showcase analytical and problem-solving skills by developing comprehensive applications and undertaking multifaceted projects to address complex challenges with Python automation.
- Instil best practices to ensure Python automation solutions are efficient and maintainable over time.

Course Curriculum

- Lesson 1: Introduction to AWS SDK for Python (Boto3)
 - Lesson 2: Automate EC2 Instance Operations
 - Lesson 3: Data Processing with AWS Lambda and Python
 - Lesson 4: Web Scraping and Data Storage on DynamoDB
 - Lesson 5: Automation with AWS Step Functions
 - Lesson 6: Stream Data Processing with Amazon Kinesis
 - Lesson 7: Chatbot Creation with Amazon Lex
 - Lesson 8: Image Analysis using Amazon Rekognition
 - Lesson 9: Automate ETL Jobs with AWS Glue
 - Lesson 10: Infrastructure as Code with AWS CDK and Python
-

Unit 36: Python Selenium II

The course "Python Selenium II" is designed to equip learners with advanced knowledge and practical skills in web automation using Python and Selenium. It delves into the integration of Python Selenium with Amazon Web Services (AWS), enabling students to automate web-based applications within a cloud environment. By the end of this course, students will not only be proficient in Python Selenium but also capable of harnessing AWS services for scalable, secure, and efficient automation. The course emphasises hands-on learning, enabling learners to apply their knowledge in real-world scenarios. The key learning objectives of this course are aimed at providing a comprehensive understanding of Python Selenium and AWS integration for web automation.

Key Learning Objectives:

- Students will learn how to provision and configure AWS resources, ensuring they are ready for Selenium testing.
- Learners will gain the skills to create and run basic Selenium tests on AWS EC2 instances, utilising cloud resources effectively.
- This objective focuses on the integration of Selenium tests into AWS's Continuous Integration/Continuous Deployment (CI/CD) pipeline, ensuring efficient and automated testing.
- Students will explore the power of parallel test execution by leveraging AWS Lambda functions.
- Learners will learn how to simulate and test for real-world load scenarios using Selenium in combination with Amazon Elastic Container Service (ECS).
- This objective emphasises the secure management of sensitive test data using AWS Secrets Manager.
- Students will acquire the skills to visualise and interpret Selenium test data using AWS Quicksight, enhancing their ability to make data-driven decisions.
- Focus on running Selenium tests in a Kubernetes environment on AWS through Amazon Elastic Kubernetes Service (EKS).
- Learners will explore infrastructure provisioning through AWS CloudFormation, streamlining the setup of testing environments.

- Learn how to leverage AWS X-Ray for advanced test debugging and monitoring in the cloud.

Course Curriculum:

- Lesson 1: Setting Up Your Environment
- Lesson 2: Automated Testing in the Cloud
- Lesson 3: Continuous Integration with AWS CodePipeline and Selenium
- Lesson 4: Parallel Test Execution with AWS Lambda
- Lesson 5: Load Testing with Selenium and Amazon ECS
- Lesson 6: Secure Test Data with AWS Secrets Manager
- Lesson 7: Analysing Test Metrics with AWS Quicksight
- Lesson 8: Containerized Testing with Amazon EKS
- Lesson 9: Infrastructure as Code with AWS CloudFormation
- Lesson 10: Advanced Debugging & Monitoring with AWS X-Ray

Unit 37: JIRA with Python II

In this course, participants will embark on a comprehensive journey into the realms of DevOps, SysOps, and AI, focusing on the intricate integration of JIRA and Cloud technologies.

Key Learning Objectives

- Provide participants with an extensive grasp of JIRA's core functionalities and administration, ensuring they become proficient in utilising JIRA as a powerful project management tool.
- Enable learners to implement Agile methodologies within JIRA, fostering efficient project management practices that align with industry standards.
- Empower participants to create customised dashboards in JIRA, allowing them to visualise project progress and performance metrics effectively.
- Deepen participants' understanding of JIRA's search and filter capabilities, enabling them to extract valuable insights from project data efficiently.
- Immerse participants in the intricacies of AWS cloud services, providing them with the knowledge and skills to configure a JIRA ecosystem within an AWS cloud environment.
- Explore the integration of automation processes via AWS Lambda, enhancing JIRA's capabilities for automated task execution and management.
- Equip participants with the ability to leverage Python scripting within AWS infrastructure to further extend and customise JIRA functionalities.

Course Curriculum

- Lesson 1: Setting Up a JIRA Instance on AWS EC2
- Lesson 2: AWS RDS Database Integration with JIRA
- Lesson 3: Automating JIRA Backups using AWS Lambda
- Lesson 4: Setting Up JIRA Service Desk with Amazon Connect

- Lesson 5: Scaling JIRA with AWS Auto Scaling and Load Balancers
 - Lesson 6: Monitoring JIRA using Amazon CloudWatch
 - Lesson 7: JIRA Data Migration using AWS Data Migration Service (DMS)
 - Lesson 8: Enhancing Security with AWS Key Management Service (KMS)
 - Lesson 9: JIRA Integration with AWS Systems Manager for Patch Management
 - Lesson 10: Implementing AWS CodePipeline for JIRA Customization
-

Unit 38: Python Flask II

The course "Python Flask II" is an advanced exploration of Python Flask development, focusing on its integration with DevOps, SysOps, and AI technologies. This comprehensive program aims to equip learners with an in-depth understanding of Flask, advanced API engineering, optimised database connectivity, integration with external systems, cutting-edge session management, and deployment strategies using Docker. Additionally, it delves into advanced AWS cloud practices, including AWS Elastic Beanstalk, RDS, AWS Lambda, and API Gateway, to help learners effectively architect cloud resources to support Flask applications.

Key Learning Objectives:

- Gain a profound understanding of Python Flask development.
- Emphasise advanced capabilities and integration with cloud solutions.
- Master the engineering of advanced APIs with Flask.
- Learn complex functionalities and integration techniques.
- Explore the nuances of optimised database connectivity within the Flask environment.
- Ensure efficient data management.
- Develop expertise in integrating complex external systems, such as Jira, to enhance Flask applications' functionality.
- Delve into the development of cutting-edge session management techniques to enhance user experiences.
- Master deployment strategies using Docker containers.
- Prepare learners to tackle real-world deployment challenges effectively.
- Engage in advanced AWS cloud practices through hands-on labs.
- Cover AWS Elastic Beanstalk, RDS, AWS Lambda, and API Gateway.
- Learn to architect cloud resources effectively to support Flask applications.

Course Curriculum:

- Lesson 1: Flask Microservices Deployment on AWS ECS
- Lesson 2: Infrastructure as Code with AWS CDK and Flask
- Lesson 3: Continuous Deployment with Flask using AWS CodePipeline & CodeBuild
- Lesson 4: Monitoring Flask Apps using Amazon CloudWatch
- Lesson 5: Database Migration and Backups with Flask using AWS DMS and RDS
- Lesson 6: Advanced Session Management with Flask and AWS ElastiCache
- Lesson 7: Serverless Flask Applications with AWS Lambda and API Gateway

- Lesson 8: Infrastructure Monitoring with Flask, AWS Config, and AWS Systems Manager
 - Lesson 9: Auto-Scaling Flask Applications on AWS with Load Balancers
 - Lesson 10: Secure Flask Deployment with AWS WAF and AWS Shield
-

Unit 39: Vagrant II

The "Vagrant II" course is designed to empower learners with advanced expertise in cloud-native AWS technologies while aligning with DevOps and SysOps methodologies. In this comprehensive program, participants will embark on a journey that encompasses the mastery of AWS cloud-native solutions, hands-on skill development, automation proficiency, and strategic adaptation. By the end of this course, learners will be well-equipped to excel in cloud technology and operations careers, with a deep understanding of AWS, DevOps, and SysOps practices.

Key Learning Objectives:

- Gain in-depth knowledge of AWS cloud-native solutions, including AWS Cloud9, AWS Elastic Container Service (ECS), and AWS Lambda, enabling the ability to engineer, manage, and orchestrate scalable development workflows.
- Engage in rigorous hands-on labs and real-world scenarios to foster expertise in creating, managing, and scaling cloud-native environments within the AWS ecosystem.
- Harness AWS automation capabilities by integrating tools like AWS CodePipeline and AWS Systems Manager to automate and streamline repetitive tasks for optimal DevOps workflow management.
- Seamlessly integrate AWS cloud-native technologies with SysOps strategies, promoting efficient and resilient development lifecycles.
- Equip learners with strategic insights to adapt, innovate, and lead in the rapidly evolving cloud technology landscape, preparing them to excel as leaders in their field.

Course Curriculum:

- Lesson 1: AWS Cloud9 Environment Setup & Integration
 - Lesson 2: Containerized Development with AWS ECS
 - Lesson 3: Serverless Architectures with AWS Lambda and API Gateway
 - Lesson 4: CI/CD Pipelines with AWS CodePipeline & CodeBuild
 - Lesson 5: Infrastructure Monitoring with AWS Config and Systems Manager
 - Lesson 6: Advanced Networking with AWS VPC and PrivateLink
 - Lesson 7: Auto-Scaling and Resilience with AWS EC2 and ELB
 - Lesson 8: Log Management and Analysis with AWS CloudWatch and ElasticSearch
 - Lesson 9: Data Management and Backups using AWS RDS and DMS
 - Lesson 10: Security Best Practices with AWS IAM, KMS, and WAF
-

Unit 40: Ansible II

In this Ansible II course, learners will dive deep into the intricacies of Ansible, a leading open-source IT automation tool, within the contexts of DevOps, SysOps, and AI. The course aims to provide a comprehensive understanding of Ansible's architecture, components, and its pivotal role in modern IT automation. Participants will develop a profound grasp of Ansible's capabilities and how it facilitates automation across diverse IT environments. Additionally, this course empowers learners with the knowledge and skills to integrate Ansible with AWS, thereby harnessing the power of cloud infrastructure for advanced automation. By the end of this course, learners will be equipped with advanced Ansible skills, enabling them to excel in the domains of DevOps, SysOps, and AI, and to drive automation and efficiency within their organisations, particularly within the cloud environment.

Key Learning Objectives:

- Understand Ansible's architecture and components.
- Recognize Ansible's role in modern IT automation.
- Demonstrate the ability to create advanced Ansible playbooks.
- Apply advanced provisioning techniques using Ansible.
- Implement complex configuration management with Ansible.
- Deploy applications and orchestrate in multi-tier environments using Ansible.
- Construct and optimise advanced Ansible playbooks.
- Troubleshoot complex automation challenges in practical scenarios.
- Integrate Ansible with other DevOps tools effectively.
- Create holistic automation strategies that span the IT infrastructure lifecycle.
- Champion automation best practices.
- Initiate Infrastructure as Code (IaC) initiatives using Ansible.
- Lead optimization efforts within organisations using Ansible.

Course Curriculum:

- Lesson 1: Ansible Setup and Configuration with AWS EC2 Instances
- Lesson 2: Advanced Playbook Development for Multi-tier Applications
- Lesson 3: Dynamic Inventory Management with AWS
- Lesson 4: Integrating Ansible with AWS Systems Manager (SSM)
- Lesson 5: Secure Configuration using Ansible Vault and AWS Secrets Manager
- Lesson 6: Infrastructure as Code (IaC) with Ansible and AWS CloudFormation
- Lesson 7: Automated Continuous Deployment with Ansible and AWS CodePipeline
- Lesson 8: Monitoring and Alerts with Ansible and AWS CloudWatch
- Lesson 9: Scaling Infrastructure using Ansible and AWS Auto Scaling Groups (ASG)
- Lesson 10: Security Hardening and Compliance Auditing with Ansible

Unit 41:Kubernetes Application Developer II

The "Kubernetes Application Developer II" course is designed to provide participants with an extensive understanding of Kubernetes within the cloud-native and open-source ecosystem. This course equips learners with the knowledge and practical skills necessary to become proficient Kubernetes developers, capable of deploying, managing, and troubleshooting containerized applications seamlessly in cloud environments, with a particular focus on AWS services. The curriculum encompasses core Kubernetes concepts, AWS cloud integration, best practices for DevOps and SysOps, hands-on experience, and strategic architectural proficiency. Upon successful completion, participants will be well-prepared to excel in dynamic operational roles.

Key Learning Objectives:

- Deep understanding of core Kubernetes architectures, including pods, services, replica sets, and secrets.
- Proficiency in advanced Kubernetes constructs like Helm charts, StatefulSets, DaemonSets, and Custom Resource Definitions (CRDs).
- Expertise in integrating Kubernetes with AWS services such as Amazon EKS, RDS, S3, and AWS Lambda.
- Ability to deploy, scale, and manage containerized applications seamlessly within the AWS cloud environment.
- Knowledge of Kubernetes best practices for continuous integration and continuous deployment (CI/CD).
- Proficiency in infrastructure as code (IaC), monitoring, logging, and security aligned with DevOps and SysOps principles.
- Capability to troubleshoot complex Kubernetes deployments.
- Development of automation strategies and use of open-source toolchains for practical Kubernetes application development.
- Skills to design and manage sophisticated container orchestration solutions.
- Alignment with AWS's cloud-native offerings and the broader open-source community for strategic architectural proficiency.

Course Curriculum:

- Lesson 1: Setting Up a Kubernetes Cluster on Amazon EKS
- Lesson 2: Deploying Stateful Applications with Amazon RDS Backend
- Lesson 3: Advanced Application Deployment with Helm
- Lesson 4: Integration with AWS Lambda using Kubeless
- Lesson 5: Continuous Deployment with Jenkins and EKS
- Lesson 6: Kubernetes Monitoring with Prometheus and Grafana on AWS
- Lesson 7: Implementing Network Policies with Calico
- Lesson 8: Kubernetes Autoscaling with AWS Cluster Autoscaler
- Lesson 9: Application Logging with Fluentd and Amazon Elasticsearch
- Lesson 10: Advanced Resource Management with Custom Resource Definitions (CRDs) and Operators

Unit 42: Kubernetes and Cloud Native Associates II

The course "Kubernetes and Cloud Native Associates II" is a comprehensive journey into the world of Kubernetes and cloud-native technologies, with a focus on AWS and open-source solutions. This course is designed to equip learners with advanced skills and knowledge in Kubernetes, cloud-native infrastructure, DevOps, SysOps, networking, security, customization, multi-cloud deployments, and real-world scenarios. Participants will not only understand the theoretical constructs but also gain practical experience through hands-on labs. By the end of this course, learners will be adept cloud-native strategists, well-versed in AWS, open-source technologies, DevOps, and SysOps, enabling them to architect, deploy, and manage sophisticated cloud-native solutions effectively.

Key Learning Objectives:

- Obtain a profound understanding of cloud-native principles and architectural blueprints for scalable and resilient applications.
- Master strategic deployment, scaling, and management of applications in Kubernetes with a focus on high availability, fault tolerance, and security.
- Immerse in the DevOps paradigm within the Kubernetes ecosystem, setting up CI/CD pipelines and implementing infrastructure as code with Helm and Terraform.
- Dive into system operations in cloud-native environments, utilising tools like Prometheus, Grafana, and AWS CloudWatch for logging, tracing, and debugging.
- Decode Kubernetes networking, from basic pod communication to advanced service mesh implementations using Istio and Linkerd for secure microservices communication.
- Evaluate stateful application patterns and integrate Kubernetes with AWS RDS, Amazon S3, and open-source storage solutions.
- Cultivate advanced skills to secure Kubernetes clusters, integrating AWS security services and open-source tools like OPA for IAM, network policies, and secrets management.
- Engineer solutions using Custom Resource Definitions (CRDs), controllers, and operators for automation and extending Kubernetes capabilities.
- Strategically plan and deploy applications in multi-cloud environments, leveraging both AWS and open-source tools for seamless operation across different cloud providers.
- Engage in meticulously crafted hands-on labs that mirror real-world scenarios, addressing complex challenges and reinforcing the synergy of theory and practice.

Course Curriculum:

- Lesson 1: Cloud-Native Infrastructure and Architecture
- Lesson 2: Advanced Kubernetes Deployment and Management
- Lesson 3: DevOps in Kubernetes
- Lesson 4: SysOps and Monitoring
- Lesson 5: Networking and Service Mesh
- Lesson 6: State Management in Cloud Native
- Lesson 7: Security and Compliance
- Lesson 8: Kubernetes Extensions and Customization

- Lesson 9: Multi-cloud and Hybrid Deployments
- Lesson 10: Hands-On Labs and Real-world Scenarios

Unit 43: Kubernetes Administrator II

In the "Kubernetes Administrator II" course, learners will embark on an advanced journey in Kubernetes administration, specifically tailored for the contemporary cloud landscape. This course aims to provide a comprehensive understanding of Kubernetes administration, equipping students to harness its capabilities within the context of DevOps, SysOps, and AI practices. Through a blend of deep exploration, hands-on experience, and practical applications, learners will emerge with the skills needed to manage Kubernetes clusters proficiently and optimise their performance in dynamic cloud environments.

Key Learning Objectives:

Upon completing this course, students will have mastered the following key areas:

- Immerse learners in a comprehensive exploration of Kubernetes, delving into its architecture, components, and its critical role in modern DevOps, SysOps, and AI practices within cloud environments.
- Equip learners with the skills to proficiently deploy, manage, and maintain Kubernetes clusters, emphasising the contemporary cloud landscape.
- Foster hands-on expertise through a series of practical exercises and real-world scenarios, enabling learners to apply their knowledge in deploying and optimising Kubernetes clusters effectively.
- Highlight Kubernetes' pivotal position in facilitating seamless integration with modern development and operational workflows. Showcase its synergy with AWS cloud services and open-source tools, demonstrating its transformative impact on DevOps and SysOps practices.
- Empower learners to optimise Kubernetes clusters for performance, scalability, and resource efficiency, ensuring they can adapt and thrive in dynamic cloud environments.
- Address the ethical dimensions of deploying AI solutions within Kubernetes clusters, including responsible AI practices, data privacy, and security.

Course Curriculum:

- Lesson 1: Setting Up a Kubernetes Cluster on AWS EKS
- Lesson 2: Cluster Networking and Service Discovery
- Lesson 3: Persistent Storage Solutions with AWS EBS and OpenEBS
- Lesson 4: Advanced Cluster Monitoring with Prometheus and Grafana
- Lesson 5: Cluster Logging with Fluentd, Elasticsearch, and AWS CloudWatch
- Lesson 6: Kubernetes Autoscaling: Nodes and Pods
- Lesson 7: Securing the Cluster with Role-Based Access Control (RBAC) and AWS IAM
- Lesson 8: Implementing Continuous Deployment in Kubernetes with Jenkins and AWS CodePipeline
- Lesson 9: Cluster Backup and Disaster Recovery with Stash and AWS S3

- Lesson 10: Hybrid Deployments: Connecting On-Premises Clusters with AWS EKS using OpenVPN

Unit 44: Kubernetes Security Specialist II

The course "Kubernetes Security Specialist II" is designed to provide students with a deep understanding of Kubernetes security within cloud-native environments. It explores the convergence of DevOps, SysOps, and AI, emphasising the significance of Kubernetes security. Students will focus on AWS and open-source cloud technologies, gaining practical insights and hands-on experience. The course addresses real-world challenges and vulnerabilities specific to cloud-native deployments, enabling students to design and implement comprehensive security strategies. By the end of the course, students will emerge as proficient Kubernetes security specialists with the knowledge and skills to ensure the resilience and integrity of cloud-native ecosystems in AWS and beyond.

Key Learning Objectives:

- Demonstrate proficiency in securing Kubernetes clusters on AWS, employing best practices and AWS-native security features.
- Establish Role-Based Access Control (RBAC) within Kubernetes and integrate it with AWS IAM, ensuring proper permissions management.
- Configure network policies using Calico to effectively segment pod-to-pod communication and enhance inter-namespace traffic security in Kubernetes.
- Manage secrets in Kubernetes using native secret management and integrate with AWS Secrets Manager for enhanced security.
- Implement Pod Security Policies (PSP) and use Open Policy Agent (OPA) to enforce custom security rules at the pod level.
- Deploy Falco in the Kubernetes cluster, create custom security rules, and integrate alerts with AWS SNS.
- Deploy Istio for secure service mesh implementation, configure mTLS for service-to-service communication, and establish secure ingress and egress controls.
- Implement advanced cluster monitoring and logging for security using Prometheus for monitoring and the EFK (Elasticsearch-Fluentd-Kibana) stack for logging, and integrate with AWS CloudWatch.
- Integrate Clair with the CI/CD pipeline for vulnerability scanning of container images and leverage AWS ECR's native scanning capabilities.
- Simulate a security breach, gather forensic data, and coordinate an incident response using AWS tools like CloudTrail and Config within a Kubernetes environment.

Course Curriculum:

- Lesson 1: Kubernetes Cluster Security on AWS
- Lesson 2: Role-Based Access Control (RBAC) and AWS IAM Integration
- Lesson 3: Network Policies and Segmentation with Calico
- Lesson 4: Secret Management with AWS Secrets Manager & Kubernetes Secrets
- Lesson 5: Pod Security Policies & Open Policy Agent (OPA) Enforcement

- Lesson 6: Container Runtime Security with Falco
 - Lesson 7: Secure Service Mesh Implementation with Istio
 - Lesson 8: Advanced Cluster Monitoring & Logging for Security with Prometheus and EFK Stack
 - Lesson 9: Vulnerability Management and Image Scanning with Clair and AWS ECR
 - Lesson 10: Incident Response & Forensics in Kubernetes
-

Unit 45: AWS Solution Architecture II

The course "AWS Solution Architecture II" delves deep into the realm of Amazon Web Services (AWS) architecture, focusing on advanced and intricate aspects of cloud solutions. Students will embark on a comprehensive journey, enabling them to harness AWS capabilities for DevOps and SysOps scenarios. By the end of this course, participants will be equipped with a profound understanding of AWS Solution Architecture, allowing them to tackle complex challenges and drive architectural decisions in AWS-centric environments.

Key Learning Objectives:

By successfully completing this course, students will achieve the following key learning objectives:

- Exhibit an advanced and integrated understanding of AWS Solution Architecture principles.
- Critically appreciate the complexities and intricacies of the AWS platform in the context of DevOps and SysOps.
- Conceptualize, critique, and design scalable, secure, and cost-effective architectures tailored to specific scenarios and business requirements.
- Analyse and interpret AWS-related challenges, and devise solutions grounded in theoretical and practical insights.
- Execute sophisticated AWS architecture designs, drawing on best practices and the latest industry standards.
- Engage in comprehensive hands-on exercises to implement architectures that reflect security, compliance, and organisational needs.
- Communicate complex AWS architectural decisions effectively to both technical and non-technical stakeholders.
- Collaborate in diverse teams, driving architectural choices and adapting to the ever-evolving AWS ecosystem.

Course Curriculum:

- Lesson 1: Setting up AWS Environment with Terraform
- Lesson 2: Building Dockerized Applications on AWS
- Lesson 3: Continuous Integration with Jenkins and AWS CodePipeline
- Lesson 4: AWS Lambda & Serverless Architecture
- Lesson 5: Kubernetes Deployment on AWS EKS
- Lesson 6: Monitoring and Observability with Prometheus and Grafana
- Lesson 7: Advanced Networking with AWS VPC & Calico

- Lesson 8: Configuration Management with Ansible and AWS Systems Manager
 - Lesson 9: Database Deployment & Management with AWS RDS and PostgreSQL
 - Lesson 10: Security & Compliance with AWS Config & OpenSCAP
-

Unit 46: Microsoft Azure Administrator II

The "Microsoft Azure Administrator II" course is designed to provide students with advanced knowledge and practical skills required to excel in managing complex Azure infrastructures, with a particular emphasis on DevOps and SysOps contexts. This academically rigorous and practically grounded course delves deep into the architectural principles of the Microsoft Azure cloud platform, equipping students with the capacity to design, deploy, and manage intricate Azure-based applications and services. The course not only focuses on technical proficiency but also nurtures analytical, strategic, and decision-making skills essential for top-tier Azure architects.

Key Learning Objectives:

Upon successful completion of the course, students will have achieved the following key learning objectives:

- Gain a deep-seated understanding of architectural principles within the Microsoft Azure cloud platform and its role in modern cloud computing paradigms.
- Expertly design complex Azure infrastructures following best practices and industry standards relevant to DevOps and SysOps.
- Master the entire lifecycle management of Azure-based applications and services, from design and deployment to matured operations.
- Implement and manage complex cloud solutions, emphasising integration, scalability, resilience, and performance, addressing operational challenges specific to Azure.
- Analyse, diagnose, and rectify complex challenges across diverse Azure services to ensure optimal system reliability and user experience.
- Effectively communicate complex Azure architectural decisions in technical documentation and collaborative discussions, aligning with stakeholder needs and industry demands.

Course Curriculum:

- Lesson 1: Azure Infrastructure as Code with ARM Templates and Terraform
 - Lesson 2: Azure Kubernetes Service (AKS) Deployment and Management
 - Lesson 3: CI/CD Pipelines with Azure DevOps and GitHub Actions
 - Lesson 4: Azure Traffic Manager and Application Gateway for High Availability
 - Lesson 5: Azure Cosmos DB Clustering and Replication
 - Lesson 6: Advanced Networking with Azure Virtual WAN and VPN Gateway
 - Lesson 7: Monitoring and Diagnostics with Azure Monitor and Grafana
 - Lesson 8: Security and Identity with Azure AD and Key Vault
 - Lesson 9: Serverless Workflows with Azure Functions and Logic Apps
 - Lesson 10: Cost Management and Performance Optimization in Azure
-

Unit 47: Professional Cloud Security II

"Cloud Security Professional II" is a comprehensive course designed for IT and information security leaders seeking to excel in the dynamic and evolving landscape of cloud security. As businesses and organisations increasingly adopt complex multi-cloud infrastructures, the need for experts in securing these environments becomes imperative. This course provides learners with vendor-neutral competencies, enabling them to navigate the multifaceted challenges of cloud security, mitigate threats, and ensure optimal protection and compliance. Graduates of this course will be well-equipped to design, deploy, manage, and advocate for robust cloud security protocols.

Key Learning Objectives:

Upon successful completion of the "Cloud Security Professional II" course, participants will achieve the following key learning objectives:

- Obtain a nuanced, critical understanding of global cloud cyber threats and their implications for businesses, individuals, and societies.
- Comprehend the landscape of vendor-neutral cloud environments and the inherent security challenges and opportunities they present.
- Analyse, evaluate, and strategize comprehensive cloud security solutions, adapting to the multifaceted challenges of multi-cloud operations.
- Lead and contribute to informed debates and discussions on emerging threats, vulnerabilities, and mitigation strategies in cloud security.
- Exhibit mastery in designing, deploying, and managing secure cloud architectures, considering best practices in cloud security design, operations, and service orchestration.
- Navigate and resolve complex security issues across diverse cloud platforms, ensuring optimal protection and compliance.
- Effectively communicate and advocate for robust cloud security protocols, both in strategic planning sessions and operational implementations.
- Collaborate across interdisciplinary teams, ensuring a cohesive approach to cloud security and risk management.

Course Curriculum:

- Lesson 1: Advanced Configuration of AWS Identity and Access Management (IAM)
- Lesson 2: Centrally Manage Security with AWS Security Hub and AWS Config
- Lesson 3: Design and Implement Automated Security Responses with AWS Lambda
- Lesson 4: Architect Secure Virtual Private Cloud (VPC) Environments
- Lesson 5: Automate Patch Management with AWS Systems Manager
- Lesson 6: Secure Serverless Applications with AWS WAF
- Lesson 7: Implement and Manage Data Encryption with AWS Key Management Service (KMS)
- Lesson 8: Integrate Security Checks into DevOps Pipelines with AWS CodePipeline and Amazon GuardDuty
- Lesson 9: Secure Containerized Applications on Amazon ECS
- Lesson 10: Implement Multi-Account Security with AWS Control Tower

Unit 48: Cloud Security Standards Review II

In an era where cloud computing is becoming the linchpin of global digital infrastructure, the importance of effective and informed auditing cannot be overstated. This unit, "Cloud Security Standards Review II," is specifically designed to delve deep into the complexities of cloud auditing, ensuring a thorough understanding and application of the requisite skills.

Key Learning Objectives:

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

- Equip learners with advanced knowledge and expertise in the realm of cloud IT auditing, transcending traditional IT audit domains.
- Address and fill the existing knowledge chasm in technical education for cloud IT auditing, emphasising the distinctive nature of auditing cloud-based systems as opposed to traditional systems.
- Facilitate a seamless integration of principles covered in CSA's Certificate of Cloud Security Knowledge (CCSK) with the foundational knowledge of ISACA's accredited certifications. This holistic approach ensures a multifaceted understanding of cloud security and auditing.
- Besides theoretical knowledge, emphasise on hands-on experience and real-world scenarios to help learners comprehend the challenges and intricacies of cloud auditing. Encourage learners to critically assess, design, and implement effective audit strategies tailored for diverse cloud environments.
- Ensure that by the culmination of this unit, learners are not just theoretically informed but are also professionally poised to drive, lead, and innovate in the domain of cloud auditing.

Course Curriculum:

- Lesson 1: Introduction to AWS Audit Environment
- Lesson 2: Auditing Identity & Access Management (IAM)
- Lesson 3: Secure Data Storage Auditing
- Lesson 4: Virtual Private Cloud (VPC) Infrastructure Auditing
- Lesson 5: Auditing AWS Serverless Architectures
- Lesson 6: Monitoring and Logging in AWS
- Lesson 7: AWS Database Auditing
- Lesson 8: Compliance Checks with AWS Config Rules
- Lesson 9: Threat Detection and Incident Response
- Lesson 10: Advanced Auditing with AWS Security Hub

Unit 49: ISSAP Architecture Professional Review II

The course "ISSAP Architecture Professional Review II" is designed to provide learners with an advanced and comprehensive understanding of Information Systems Security Architecture, focusing on the domains set by ISC² for the ISSAP certification. This course is

a journey through academically rigorous and professionally relevant labs, ensuring that students not only grasp theoretical concepts but also gain practical skills needed to excel in the real world and to confidently face the ISSAP examination. By navigating through a series of modules, learners will refine their analytical, evaluative, and application-based competencies, ultimately achieving a level of knowledge expected.

Key Learning Objectives:

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

- Design and implement governance frameworks that ensure compliance and effectively manage risks in IT environments.
- Conceptualize, design, and critique various security architecture models in alignment with industry standards and organisational needs.
- Craft, deploy, and evaluate security structures for safeguarding IT infrastructure, focusing on contemporary challenges and solutions.
- Design and manage IAM structures ensuring authenticated, authorised, and auditable access across IT systems.
- Ensure the security of applications throughout their lifecycle, from development to deployment and operations.
- Design and manage architectures underpinning security operations, emphasising real-time threat management, incident response, and continuous improvement.

Course Curriculum:

- Lesson 1: Governance Framework Implementation on AWS
 - Lesson 2: Design and Evaluate a Secure Infrastructure Blueprint
 - Lesson 3: IAM Role-Based Access Control (RBAC) Model
 - Lesson 4: Application Security Using AWS Secrets Manager and AWS Lambda
 - Lesson 5: Infrastructure Security Through AWS WAF and AWS Shield
 - Lesson 6: Security Architecture Modeling with AWS Step Functions
 - Lesson 7: Automated Incident Response with AWS Lambda and Amazon SNS
 - Lesson 8: Continuous Compliance Verification using AWS Config Rules
 - Lesson 9: Application Security Pipeline with AWS CodeStar
 - Lesson 10: Security Operations Dashboard using Amazon CloudWatch and AWS Security Hub
-

Unit 50: Artificial Intelligence II

In the rapidly evolving landscape of modern IT infrastructures, Artificial Intelligence (AI) has become a pivotal technology in enhancing and optimising systems, particularly in the domains of Cloud Cyber Security, DevOps, SysOps, and Governance, Risk Management, and Compliance (GRC). This RQF Level 6 course delves deep into AI's application in these specialised areas, moving beyond traditional paradigms to equip learners with the knowledge and skills necessary to excel in these specialised domains.

Key Learning Objectives

Upon course completion, learners will have attained the following key learning objectives:

- Gain an in-depth comprehension of how AI can be leveraged to detect vulnerabilities, predict cyber-attacks, and proactively enhance threat intelligence in cloud environments.
- Understand the role of AI in automating tasks, facilitating continuous integration and deployment, and optimising resource allocation in DevOps practices.
- Acquire the ability to implement AI-driven monitoring, alerting, and system optimization strategies in complex IT operations, enhancing efficiency and reliability.
- Explore how AI can be applied in the analysis of extensive datasets to improve compliance checks, risk assessments, and governance models, ensuring adherence to evolving regulatory standards.

Course Curriculum

- Lesson 1: AI-Driven Vulnerability Detection with OpenVAS and Tensorflow
- Lesson 2: Automated CI/CD Pipeline Optimization using Jenkins and MLflow
- Lesson 3: Monitoring & Alerting with Prometheus, Grafana, and AI
- Lesson 4: NLP-driven Automated Compliance Reporting with ELK Stack
- Lesson 5: Risk Assessment with AI and OpenFAIR
- Lesson 6: Self-Healing Systems with Kubernetes and AI
- Lesson 7: AI-Enhanced Firewall Rules Optimization with pfSense and Scikit-learn
- Lesson 8: Automated Data Classification for GDPR with Python and NLP
- Lesson 9: AI-Driven Intrusion Detection with Snort and PyTorch
- Lesson 10: Application Security Enhancement using OWASP ZAP and AI

Unit 51: Python Programming for Machine Learning II

Welcome to "Python Programming for Machine Learning II," an academically rigorous course designed to enhance your Python programming skills and their application in the fields of Machine Learning, Artificial Intelligence, DevOps, SysOps, and Cloud Cyber Security. This course is intended for learners with foundational knowledge in Python and Machine Learning, aiming to deepen their understanding of advanced Python constructs and their real-world implementation. It also focuses on the secure deployment of Machine Learning-based solutions within cloud infrastructure. In this course, you will explore key topics and labs that will equip you with the skills necessary to excel in these domains.

Key Learning Objectives

By the end of this course, you will have achieved the following key learning objectives:

- Design secure cloud infrastructure using Terraform scripts, following principles of least privilege and encryption at rest and in transit.
- Create a secure CI/CD pipeline with Jenkins and GitHub, ensuring code quality and security compliance.
- Implement Role-Based Access Control (RBAC) for Kubernetes, designing and enforcing security policies.
- Monitor and analyze cloud system logs for security threats using the ELK stack.
- Implement policy checks within CI/CD pipelines to ensure Governance, Risk, and Compliance (GRC) compliance using Open Policy Agent (OPA).
- Evaluate Docker images for vulnerabilities using Clair and enhance container security.
- Create immutable server images with baked-in security configurations using Packer and Ansible.
- Design a secure network architecture on AWS using VPC and enhance Kubernetes network security using Calico.
- Monitor system and application health, focusing on security metrics, using Prometheus and Grafana.
- Develop serverless applications ensuring secure execution using AWS Lambda and AppArmor.

Course Curriculum

- Lesson 1: Secure Infrastructure as Code (IaC) with Terraform and AWS
- Lesson 2: Continuous Integration/Continuous Deployment (CI/CD) with Jenkins and GitHub
- Lesson 3: Implementing Role-Based Access Control (RBAC) with Kubernetes
- Lesson 4: Security Incident and Event Management (SIEM) with ELK Stack
- Lesson 5: Compliance as Code with Open Policy Agent (OPA)
- Lesson 6: Container Security with Docker and Clair
- Lesson 7: Immutable Infrastructure with Packer and Ansible
- Lesson 8: Network Security and Isolation with VPC and Calico
- Lesson 9: Infrastructure Monitoring with Prometheus and Grafana
- Lesson 10: Serverless Security with AWS Lambda and AppArmor

Unit 52:Deep Learning II

"Deep Learning II" is an advanced course designed to equip learners with the knowledge and skills required to implement and optimise deep learning solutions using OpenAI and AWS technologies. The course emphasises the seamless integration of these solutions within a framework that prioritises cloud security, DevOps, and SysOps best practices. In this course, students will delve into the intricacies of advanced deep learning, proficiency in AWS cloud technologies, integration with DevOps and SysOps, holistic cloud security, practical

application, and collaborative approaches. The curriculum ensures students are prepared for advanced roles in AI-driven digital ecosystems.

Key Learning Objectives:

- Develop a comprehensive understanding of OpenAI's advanced deep learning capabilities, enabling students to design, build, and enhance models for real-world applications.
- Equip learners to effectively use AWS services pertinent to deep learning, cloud infrastructure management, and security.
- Integrate deep learning workflows with DevOps and SysOps methodologies, focusing on AWS tools for automation, monitoring, continuous integration, and deployment.
- Provide an in-depth understanding of cloud security best practices on AWS, ensuring students can design and enforce stringent security policies to protect data, models, and cloud resources.
- Challenge students to develop end-to-end solutions that merge deep learning with cloud operations, addressing genuine industry challenges through hands-on projects.
- Promote teamwork and interdisciplinary collaboration, simulating real-world scenarios where data scientists, cloud architects, and security professionals must work in tandem.

Course Curriculum:

- Lesson 1: Introduction to OpenAI and AWS Integration
- Lesson 2: Automated Deep Learning Workflows with AWS CodePipeline
- Lesson 3: Secure Model Deployment with AWS Secrets Manager
- Lesson 4: Deep Learning at Scale with AWS Elastic Kubernetes Service (EKS)
- Lesson 5: Data Security and Encryption with AWS
- Lesson 6: Monitoring with AWS CloudWatch and OpenAI Logs
- Lesson 7: Resilient Deployments with AWS Lambda and Auto Scaling
- Lesson 8: Infrastructure as Code with AWS CloudFormation
- Lesson 9: Model A/B Testing on AWS SageMaker
- Lesson 10: Ethical and Privacy Considerations in Deployments

Unit 53: Machine Learning - Mathematics and Python Implementation II

The course "Machine Learning - Mathematics and Python Implementation II" is a comprehensive exploration of the foundational mathematical principles behind machine learning algorithms, combined with hands-on Python implementation within the context of Cloud Security, DevOps, and SysOps best practices. This course aims to empower learners with a deep understanding of the mathematical concepts underpinning machine learning, the proficiency to implement machine learning algorithms using Python, and the ability to securely integrate machine learning solutions within cloud architectures while adhering to best practices in Cloud Security.

Key Learning Objectives:

- Develop a profound understanding of the mathematical concepts, including linear algebra, calculus, statistics, and probability, that drive various machine learning algorithms.
- Acquire adeptness in using Python and its key libraries, such as NumPy, SciPy, and Scikit-learn, to implement and experiment with machine learning algorithms from scratch.
- Learn to integrate machine learning implementations securely within cloud architectures, emphasising data encryption, model protection, and access controls.
- Seamlessly integrate machine learning workflows with DevOps and SysOps methodologies, focusing on automation, monitoring, continuous integration, deployment, and infrastructure management.
- Develop a practical, application-driven approach by addressing industry challenges, ensuring a match between mathematical understanding and hands-on coding experience.
- Highlight the importance of ethical considerations in machine learning, focusing on data privacy, model fairness, and compliance within cloud-based deployments.

Course Curriculum:

- Lesson 1: Setting Up a Secure Machine Learning Environment with Python
- Lesson 2: Linear Algebra Essentials with NumPy
- Lesson 3: Calculus in Machine Learning with SciPy
- Lesson 4: Probability and Statistics with Python
- Lesson 5: Implementing a Decision Tree Algorithm from Scratch
- Lesson 6: Cloud Security: Data Encryption and Model Protection
- Lesson 7: Continuous Integration and Deployment for ML using Jenkins
- Lesson 8: Monitoring and Scaling ML Workflows with Kubernetes
- Lesson 9: Infrastructure as Code with Terraform for ML Deployments
- Lesson 10: Ethical Considerations in Machine Learning using Fairness Indicators

Unit 54: Advanced topics in Machine Learning II

The course, "Advanced Topics in Machine Learning II," is designed to provide learners with an in-depth understanding of cutting-edge machine learning methodologies and their integration into cloud environments. Emphasising best practices in DevOps and SysOps, this course equips students with the skills necessary to deploy and operate machine learning models securely in cloud platforms. All content is grounded in open-source technologies to foster accessibility, transparency, and collaborative adaptability.

Key Learning Objectives:

- Delve into the world of cutting-edge machine learning algorithms, techniques, and strategies, empowering learners to address complex, real-world challenges with innovative solutions.
- Impart the significance of cloud security, focusing on best practices in data protection, secure model deployment, and robust access controls for machine learning applications.
- Equip students with the knowledge to seamlessly integrate machine learning workflows with DevOps methodologies, such as CI/CD, while ensuring system reliability through SysOps practices.
- Guide learners in optimising machine learning solutions for scalability in cloud environments, ensuring efficiency in both model training and inference.
- Encourage hands-on experimentation and collaboration using open-source machine learning frameworks and tools, fostering a community-driven learning approach.
- Stress the importance of ethically developing machine learning models, addressing issues of bias, transparency, and fairness, particularly in cloud environments.

Course Curriculum:

- Lesson 1: Initialise a Safe Environment for ML
- Lesson 2: Introduction to GANs and TensorFlow
- Lesson 3: Deploying ML Models with Kubernetes
- Lesson 4: Automating ML Workflows with Apache Airflow
- Lesson 5: Advanced Cloud Security with SPIFFE
- Lesson 6: Integrating ML with DevOps using GitLab CI/CD
- Lesson 7: Exploring Reinforcement Learning with OpenAI Gym
- Lesson 8: Deep Dive into NLP with HuggingFace Transformers
- Lesson 9: Scaling ML with Distributed Training using Horovod
- Lesson 10: Ensuring Ethical AI with SHAP

Unit 55: Practical Applications of Machine Learning II

The course "Practical Applications of Machine Learning II" is designed to provide learners with an in-depth understanding of how machine learning can be applied to real-world challenges in the domains of Cloud Security, Cyber Security, DevOps, and SysOps. This course goes beyond theory, focusing on hands-on, practical skills, and leveraging open-source technologies to address contemporary issues in security and operations, with the integration of machine learning. The course aims to prepare students for advanced roles in industries where machine learning intersects with cloud, cyber, DevOps, and SysOps.

Key Learning Objectives:

By the end of this course, learners will have achieved the following key learning objectives:

- Understand how machine learning algorithms can detect, predict, and mitigate cyber threats and anomalies.
- Dive deep into machine learning applications to ensure data integrity, confidentiality, and availability in cloud environments.

- Learn how machine learning can improve CI/CD pipelines, automate testing, and enhance deployment strategies.
- Understand how machine learning can monitor system health, predict failures, and automate routine tasks.
- Employ open-source machine learning frameworks and tools to ensure transparent, flexible, and collaborative solutions.
- Study the ethical considerations of implementing machine learning in security and operations, emphasising data privacy, fairness, and transparency.

Course Curriculum:

- Lesson 1: Anomaly Detection for Network Security with Scikit-learn
- Lesson 2: Cloud Data Encryption with TensorFlow
- Lesson 3: Automated Threat Intelligence with ELK Stack
- Lesson 4: CI/CD Pipeline Enhancement with Jenkins and ML
- Lesson 5: SysOps Alert Forecasting with Prophet
- Lesson 6: Intrusion Detection with Snort and ML
- Lesson 7: Real-time Security Log Analysis with Kafka and ML
- Lesson 8: Image-Based Authentication using Convolutional Neural Networks (CNN)
- Lesson 9: Automating Security Patch Testing with ML
- Lesson 10: Ethics & Fairness in Security ML Models with AI Fairness 360

Unit 56: Deep Learning Open Source Perspective

The course, "Deep Learning Open Source Perspective," offers a comprehensive exploration of advanced deep learning techniques and their integration with open-source technologies. This program is designed to empower learners with the knowledge and practical expertise to develop, deploy, and maintain cutting-edge deep learning models. Leveraging open-source tools, cloud security best practices, DevOps, and SysOps methodologies, this course provides students with a holistic understanding of the intricacies of deploying advanced deep learning solutions. The course employs a variety of teaching methods, including recorded lectures, live classes, hands-on labs, quizzes, and oral presentations, ensuring a dynamic and engaging learning experience.

Key Learning Objectives:

- Equip students with the knowledge and practical expertise to design, implement, and optimise state-of-the-art deep learning algorithms, particularly in complex environments.
- Ensure students can proficiently navigate and deploy solutions using leading open-source platforms and tools pertinent to deep learning, cloud, and systems operations.
- Embed an understanding of DevOps and SysOps principles and practices, emphasising automation, containerization, continuous integration, and continuous deployment (CI/CD) within the deep learning workflow.
- Cultivate a deep understanding of cloud security best practices. Ensure students can design and implement security protocols for deep learning applications, safeguarding data, models, and cloud infrastructure against potential threats.

- Through practical labs, challenge students to solve real-world problems by integrating deep learning with cloud, security, and operations, reflecting scenarios they may encounter in industry settings.
- Encourage collaborative problem-solving and team-based projects, simulating the interdisciplinary nature of deploying deep learning solutions in a corporate ecosystem.
- Foster awareness of ethical concerns related to deploying deep learning in cloud environments, emphasising data privacy, model transparency, and fairness.

Course Curriculum:

- Lesson 1: Setting Up the Environment
- Lesson 2: Automated Deep Learning Model Training with CI/CD
- Lesson 3: Containerized Deep Learning Deployment
- Lesson 4: Cloud-based Model Training with GPU Acceleration
- Lesson 5: Deep Learning Model Security in the Cloud
- Lesson 6: Continuous Monitoring and Logging with ELK Stack
- Lesson 7: Automated Scaling with Cloud Functions and Serverless Architecture
- Lesson 8: Multi-Model Deployment and A/B Testing
- Lesson 9: Resilient Deep Learning Architectures with Failover Strategies
- Lesson 10: Ethical and Fair AI in Practice

Unit 57: Machine learning Model Development and Deployment II

Welcome to Machine Learning Model Development and Deployment II, an advanced course designed to deepen your expertise in developing, refining, and deploying machine learning models. This course is tailored to address the intricate demands of contemporary IT ecosystems, focusing on key areas such as cybersecurity, cloud security, DevOps, and SysOps. By leveraging open-source technologies, we aim to foster innovation, collaboration, and transparency within the realm of machine learning. As you progress through this course, you will encounter challenges that mimic real-world scenarios, helping you bridge the gap between machine learning and operational requirements, as well as security challenges.

Key Learning Objectives:

- Delve into the nuances of constructing robust, efficient, and versatile machine learning models tailored for complex use-cases.
- Harness the potential of ML models to predict, detect, and remediate cyber threats and vulnerabilities in real-time.
- Understand the intricacies of embedding machine learning models into cloud infrastructure to enhance data security, integrity, and availability.
- Incorporate machine learning into the CI/CD pipeline, focusing on automating, optimising, and enhancing DevOps processes.

- Use machine learning to streamline SysOps tasks, including predictive maintenance, system health monitoring, and automated issue resolution.
- Develop proficiency in using open-source machine learning tools, frameworks, and platforms to ensure solutions are transparent, adaptable, and community-driven.
- Gain expertise in deploying machine learning models into production environments securely and efficiently, adhering to best practices and industry standards.

Course Curriculum:

- Lesson 1: Advanced Cyber Threat Detection with Open-source ML Frameworks
- Lesson 2: Secure Cloud Data Storage with ML-enhanced Encryption
- Lesson 3: ML-driven Continuous Integration (CI) in DevOps
- Lesson 4: SysOps System Health Prediction with Time Series Analysis
- Lesson 5: Real-time Anomaly Detection in Cloud Infrastructure
- Lesson 6: ML-enhanced Intrusion Detection System (IDS) with Snort
- Lesson 7: Optimising SysOps with Predictive Maintenance ML Models
- Lesson 8: Machine Learning in SecDevOps - Security Scanning Automation
- Lesson 9: Deploying Scalable ML Models in Cloud with Kubernetes
- Lesson 10: Ethics, Transparency, and Bias in ML Deployment

Unit 58: Computer Vision II

The course "Computer Vision II" is a comprehensive exploration of computer vision's pivotal role in domains such as cybersecurity, cloud security, DevOps, and SysOps. Rooted in open-source technology, this course bridges the gap between visual data processing and its applications in safeguarding and optimising digital infrastructures. Through a combination of theoretical concepts and hands-on practical applications, students will gain the knowledge and skills to leverage computer vision technologies to detect vulnerabilities, enhance security measures, and streamline operational workflows in diverse IT environments. This course not only equips learners with a strong theoretical foundation but also empowers them to apply these concepts using open-source tools and platforms.

Key Learning Objectives:

- Gain a solid understanding of core concepts, methodologies, and techniques essential to computer vision, including image and video processing, feature extraction, and object recognition.
- Explore how computer vision can aid in real-time threat detection, enhance biometric security, and optimise surveillance systems.
- Examine the application of computer vision in ensuring data integrity, monitoring cloud resources, and detecting anomalies through visual cues.
- Investigate the role of computer vision in Continuous Integration/Continuous Deployment (CI/CD) pipelines, particularly in automating visual Quality Assurance (QA) checks and integrating visual feedback mechanisms.
- Learn how to use computer vision in system operations to monitor hardware health, streamline visual system logs, and predict system downtimes based on visual patterns.

- Develop proficiency in open-source computer vision frameworks like OpenCV and SimpleCV, fostering a collaborative and transparent approach to solution development.

Course Curriculum:

- Lesson 1: Introduction to OpenCV for Computer Vision
- Lesson 2: Real-time Surveillance with Motion Detection
- Lesson 3: Face Detection for Cybersecurity Applications
- Lesson 4: Biometric Security – Iris Recognition
- Lesson 5: Cloud Image Data Anomaly Detection
- Lesson 6: Automated Visual QA in DevOps
- Lesson 7: SysOps System Health Monitoring with Thermal Imaging
- Lesson 8: Optical Character Recognition (OCR) for Log Analysis
- Lesson 9: Cloud Security – Visual Firewall Monitoring
- Lesson 10: Real-time Video Processing with GPU Acceleration

Unit 59: Natural Language Processing II

The course "Natural Language Processing II" delves deep into the interdisciplinary field of Natural Language Processing (NLP), exploring its profound relevance and potential applications in areas such as cybersecurity, cloud security, DevOps, and SysOps. In today's digital landscape, textual data is ubiquitous, making the ability to process, understand, and extract actionable insights from this data increasingly critical. This course is designed to equip students with both the theoretical knowledge and practical skills necessary to harness NLP technologies to enhance security protocols, optimise cloud operations, and improve development and system operations workflows. Rooted in a commitment to open-source paradigms, this course encourages a transparent, collaborative, and innovative approach to problem-solving.

Key Learning Objectives:

- Introduce the core concepts, algorithms, and tools pivotal to Natural Language Processing, from tokenization to semantic analysis.
- Understand the role of NLP in parsing vast logs, detecting phishing attempts through textual content, and automatically categorising threat intelligence reports.
- Explore the potential of NLP in monitoring cloud environments, detecting anomalies through textual logs, and ensuring compliance through automated document checks.
- Investigate the application of NLP in streamlining development operations, including automating requirement analysis, processing user feedback, and ensuring documentation quality.
- Discover how to employ NLP for system operations, such as parsing system logs, automating incident reports, and predicting system downtimes through textual patterns.

- Cultivate proficiency in open-source NLP tools and libraries, such as NLTK, spaCy, and OpenNLP, and understand their integration points in the broader cybersecurity and DevOps ecosystems.

Course Curriculum:

- Lesson 1: Introduction to NLP with NLTK
 - Lesson 2: Textual Log Parsing and Analysis
 - Lesson 3: Phishing Email Detection
 - Lesson 4: Cloud Environment Monitoring through Text Analysis
 - Lesson 5: Automating Requirement Analysis in DevOps
 - Lesson 6: Processing User Feedback in SysOps
 - Lesson 7: OpenNLP for Threat Intelligence Reports
 - Lesson 8: Documentation Quality Assurance in DevOps
 - Lesson 9: Automated Incident Reporting in SysOps
 - Lesson 10: Advanced NLP with BERT for Security
-

Unit 60: 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 61: 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**

