AWS CLOUD INSTITUTE

AWS Cloud Institute: Cloud Operations 1 Syllabus

Course Overview

In this course, you will get an opportunity to develop systems management skills, understand the purpose and benefits of logging and scaling, and explain the guiding principles and methodologies of DevOps. You will start the course by learning the differences between scalability and elasticity and identifying AWS logging and scaling services. The course will introduce you to Bash shell scripts, Power Shell, and the basic constructs of scripting. You will be able to define and discuss the purpose of AWS Command Line Interface (AWS CLI) and develop functional knowledge of Amazon CloudWatch, AWS CloudTrail, and Amazon EventBridge.

Instructor-Led Training (ILT) Sessions

Attendance at ILT sessions is strongly encouraged, but attendance does not count toward course completion. You can use the ILT sessions to explore concepts presented in the online learning content in greater depth, connect with AWS instructors and ACI learners, and prepare for the weekly final assessment. All ILT sessions, with the exception of office hours, are recorded and will be available on-demand for you to watch when you have time. Multiple live ILT sessions are offered each day to accommodate a range of schedules.

Prerequisites

Introduction to Cloud Foundations

Course Completion Requirements

At the end of each week's assigned module, you will complete a multiple-choice final assessment. You have unlimited opportunities to achieve a passing score on each final assessment. You must complete the weekly final assessments with a score of 85% or higher to receive credit for the course. ILT attendance or watching ILT recordings is strongly encouraged but is not required for course completion.

Week 1: Logging and Scaling – Part 1

Goal:

Gain knowledge of the purpose and benefits of logs. Identify AWS logging and monitoring services and learn how to apply them to optimize infrastructure management and performance.

Learning Objectives:

- Describe the types of logs and the importance of logging.
- Describe the monitoring features of Amazon CloudWatch.
- Describe the benefits of creating a monitoring plan and defining monitoring goals.
- Compare two ways of monitoring instances: using the Amazon Elastic Compute Cloud (Amazon EC2) console and using the CloudWatch dashboard.
- Describe the benefits of monitoring with AWS CloudTrail.
- Describe CloudWatch features for monitoring and troubleshooting.
- Describe AWS X-Ray and how X-Ray works with CloudWatch.

- Define high-resolution metrics and composite alarms and describe how CloudWatch uses alarms to invoke scaling.

Module Outline:

1. **Logging and Monitoring in AWS**
    a. Introduction: Logging and Monitoring in AWS
    b. Logging Overview
    c. Monitoring with CloudWatch
    d. Determining a Monitoring Strategy
    e. Establishing a Baseline with Amazon EC2 Metrics
    f. Monitoring with the CloudWatch Agent
    g. Dashboards for Monitoring EC2 Instances
    h. Logging Activities with CloudTrail
    i. Knowledge Check
2. **Monitoring Application Health**
    a. Introduction: Monitoring Application Health
    b. Keeping Your Applications Healthy
    c. Serverless Observability
    d. CloudWatch Container Insights
    e. CloudWatch Application Insights
    f. CloudWatch Anomaly Detection
    g. CloudWatch Metric Streams
    h. AWS X-Ray
    i. Knowledge Check
3. **CloudWatch for Health, Availability, and Security**
    a. Introduction: CloudWatch for Health, Availability, and Security
    b. CloudWatch Dashboards
    c. CloudWatch Synthetics and CloudWatch RUM
    d. CloudWatch Logs Insights
    e. CloudWatch Metrics Insights
    f. Lab: Collecting and Analyzing Logs with Amazon CloudWatch Logs Insights
    g. CloudWatch Contributor Insights for Security
    h. Amazon CloudWatch Evidently
    i. Lab: Monitoring Security with Amazon CloudWatch
    j. High-Resolution Metrics and Alarms and Composite Alarms
    k. Scaling with CloudWatch Alarms
    l. Knowledge Check

Hands-on Labs:

- **Lab: Collecting and Analyzing Logs with Amazon CloudWatch Logs Insights (45 min)**
    - In this lab, you learn to use Amazon CloudWatch Logs Insights to interactively search and analyze log data in Amazon CloudWatch Logs. You set up log groups and log streams in CloudWatch Logs and run queries against Amazon Virtual Private Cloud (Amazon VPC) flow logs and database logs to detect potential security vulnerabilities.

- **Lab: Monitoring Security with Amazon CloudWatch (45 min)**
    - In this lab, you will monitor security on the database server with Amazon CloudWatch. You configure the database server to send log files to Amazon CloudWatch. You then create CloudWatch alarms and notifications to alert you to a specified number of login failures on your database server. Finally, you create a CloudWatch alarm and notification to monitor outgoing traffic through a NAT gateway.

Week 2: Logging and Scaling – Part 2

Goal:

Gain knowledge of the purpose and benefits of logs. Identify AWS logging and monitoring services and learn how to apply them to optimize infrastructure management and performance.

Learning Objectives:

- Describe how auto scaling works.
- Discuss auto scaling with Amazon Elastic Container Service (Amazon ECS), Amazon DynamoDB, Amazon Aurora, and Amazon EC2.
- Describe different scaling policies.
- Identify necessary services to auto scale through case studies.
- Describe launch templates for Amazon EC2 Auto Scaling.
- Explain how automatic scaling works for Amazon EC2 Spot Fleet.
- Explain how AWS Elastic Beanstalk works with an Amazon EC2 Auto Scaling group.
- Explain how to use lifecycle hooks and AWS Lambda functions to create fully managed auto scaling.
- Discuss predictive scaling for Amazon EC2 with machine learning.
- Explain how Elastic Load Balancing (ELB) works and identify the types of ELB load balancers.
- Discuss deployment strategies on AWS and identify the type of deployment by its characteristics.
- Describe how to use load balancers for blue/green and canary deployments.
- Discuss how ELB works with Amazon Route 53.
- Describe how to use AWS PrivateLink to connect ELB services.

Module Outline:

1. **Auto Scaling**
    a. Introduction: Auto Scaling
    b. How Auto Scaling Works
    c. Auto Scaling with Amazon ECS
    d. Auto Scaling with DynamoDB
    e. Auto Scaling with Aurora
    f. Amazon EC2 Auto Scaling
    g. Automatic and Manual Scaling
    h. Lab: Introduction to Amazon EC2 Auto Scaling
    i. Auto Scaling Case Studies
    j. Knowledge Check
2. **Amazon EC2 Auto Scaling Optimization**
    a. Introduction: Amazon EC2 Auto Scaling Optimization
    b. Launch Templates

   c. Spot Fleets and Auto Scaling
   d. Amazon EC2 Auto Scaling Group for Elastic Beanstalk
   e. Creating Fully Managed Auto Scaling with Lifecycle Hooks
   f. Predictive Scaling for Amazon EC2 Auto Scaling with Machine Learning
   g. Knowledge Check

3. **Elastic Load Balancing**
   a. Introduction: Elastic Load Balancing
   b. How Elastic Load Balancing Works
   c. Elastic Load Balancing Services
   d. Availability Zones and Load Balancer Nodes
   e. Deployment Strategies
   f. Activity: Identifying the Type of Deployment by its Characteristics
   g. Using an Application Load Balancer for Canary and Blue/Green Deployments
   h. Lab: Introduction to Elastic Load Balancing
   i. How Elastic Load Balancing Integrates with Route 53
   j. Using PrivateLink to Connect with Elastic Load Balancing Services
   k. Knowledge Check

Hands-on Labs:

- **Lab: Introduction to Amazon EC2 Auto Scaling (60 min)**
  - In this lab, you create a launch template that defines your Amazon Elastic Compute Cloud (Amazon EC2) instances and an Amazon EC2 Auto Scaling group with a single instance in it. You then terminate the instance and verify that the instance was removed from service and replaced. To maintain a constant number of instances, Amazon EC2 Auto Scaling automatically detects and responds to Amazon EC2 health and reachability checks.
- **Lab: Introduction to Elastic Load Balancing (60 min)**
  - In this lab you create, configure, and test a Network Load Balancer and an Application Load Balancer.

Week 3: Security, Monitoring and Compliance – Part 1

Goal:

Gain applicable knowledge of compliance and monitoring basics, and develop skills to differentiate between Amazon CloudWatch, AWS CloudTrail, Amazon EventBridge, and AWS Config.

Learning Objectives:

- Describe compliance and regulations.
- Discuss common regulations in cloud software development.
- Compare the similarities and differences of Amazon CloudWatch, AWS CloudTrail, Amazon EventBridge, and AWS Config.
- Describe the key CloudWatch concepts.
- Describe when and how to publish custom metrics to CloudWatch.
- Describe use cases for CloudWatch logs and alarms.
- Create OpsItems from a CloudWatch alarm.
- Use CloudWatch alarms and metrics.

- Describe the key CloudTrail concepts.
- Describe use cases for CloudTrail.
- Interpret CloudTrail logs.

Module Outline:

1. **Understanding Compliance and Regulations**
    a. Introduction: Understanding Compliance and Regulations
    b. Compliance and Regulations
    c. Compliance with AWS
    d. Vulnerabilities, Threats, and Weaknesses
    e. Frameworks and Standards
    f. Considerations with AnyCompany
    g. Knowledge Check
2. **AWS Tools for Monitoring and Responding**
    a. Introduction: AWS Tools for Monitoring and Responding
    b. AWS Services and Features
    c. Knowledge Check
3. **Using CloudWatch**
    a. Introduction: Using CloudWatch
    b. CloudWatch Deep Dive
    c. CloudWatch Metrics to Monitor for Security and Compliance
    d. Using CloudWatch Alarms
    e. Lab: Security Monitoring with CloudWatch Alarms
    f. Using CloudWatch Logs
    g. Activity: CloudWatch Alarm and Logs Use Case
    h. Knowledge Check
4. **Using CloudTrail**
    a. Introduction: Using CloudTrail
    b. CloudTrail Deep Dive
    c. Working with CloudTrail Logs
    d. Lab: Enabling Traceability Through CloudTrail
    e. Lab: Monitoring and Alerting with CloudTrail and CloudWatch
    f. CloudTrail Use Cases
    g. Knowledge Check

Hands-on Labs:

- **Lab: Security Monitoring with CloudWatch Alarms (45 min)**
    - In this lab, you create a CloudWatch alarm that initiates when the Amazon EC2 instance exceeds a specific CPU utilization threshold. You create a subscription using Amazon SNS that emails you if this alarm goes off. You log in to the Amazon EC2 instance and run a stress test command that causes the CPU utilization of the EC2 instance to reach 100 percent.
- **Lab: Enabling Traceability Through CloudTrail (60 min)**
    - In this lab, you learn to enable the traceability design principle. You also learn how to use cloud controls like CloudTrail, security groups, and Systems Manager to secure the cloud architecture.
- **Lab: Monitoring and Alerting with CloudTrail and CloudWatch (60 min)**

- In this lab, you will configure logging and monitoring in an AWS account. You will understand how to create a trail in CloudTrail, which will be an audit log of API calls made in the account. You will then create an Amazon SNS topic. By subscribing your email to the topic, you will be alerted when particular events occur. Next, you will create a CloudWatch alarm to notice whenever multiple failed login attempts occur for the AWS Management Console.

Week 4: Security, Monitoring, and Compliance – Part 2

Goal:

Gain a foundational knowledge of Amazon EventBridge and the attributes of AWS Config.

Learning Objectives:

- Describe key EventBridge concepts.
- Discuss default, custom, and partner event buses.
- Use event patterns and trigger rules.
- Archive and replay events.
- Discuss how decoupling services increases security.
- Describe AWS Config's key concepts.
- Create configuration snapshots.
- Discuss AWS Config integrations.
- Use AWS Config to monitor the compliance of resources.

Module Outline:

1. **Using Amazon EventBridge**
    a. Introduction: Using EventBridge
    b. EventBridge Deep Dive
    c. Understanding Event Buses
    d. Using Event Buses
    e. Lab: Utilizing EventBridge
    f. Using API Destinations
    g. Demo: Archiving and Replaying EventBridge Events
    h. EventBridge Schemas
    i. PutEvents API
    j. Establishing Global Endpoints
    k. Amazon EventBridge Use Cases
    l. Knowledge Check
2. **Using AWS Config**
    a. Introduction: Using AWS Config
    b. AWS Config Deep Dive
    c. Using Aggregators with AWS Config and AWS Organizations
    d. Using AWS Config Conformance Packs and Scores
    e. Delivering and Viewing Configuration Snapshots
    f. Integrating with AWS Config
    g. Lab: Automating Compliance and Security with AWS Config
    h. Lab: Auditing AWS Resources with Systems Manager and AWS Config

   i. Activity: AWS Config Use Cases
   j. Knowledge Check

Hands-on Labs:

- **Lab: Utilizing EventBridge (40 min)**
   - In this lab, you will create Lambda functions to log events and reboot EC2 instances, enable EventBridge to log auto scaling events, create an EventBridge Schedule to reboot EC2 instances monthly, and test an EventBridge rule by manually updating the Auto Scaling group.
- **Lab: Automating Compliance and Security with AWS Config (60 min)**
   - In this lab, you will learn how to set up AWS Config, view your resource inventory, create compliance rules, and remediate resources that are noncompliant. You will learn to define security rules and compliance requirements, monitor infrastructure against the rules and requirements, detect violations, rapidly act on violations with automation.
- **Lab: Auditing Your AWS Resources with Systems Manager and AWS Config (60 min)**
   - In this lab, you will set up processes for both AWS Config and Systems Manager Inventory in an AWS environment with EC2 instances. AWS Config and Systems Manager are services that aid a CloudOps engineer in monitoring and remediating compliance tasks.

Week 5: Systems Management – Part 1

Goal:

This module introduces the learner to systems management skills from the perspective of a cloud application developer and the services that AWS offers for systems management support. It offers an overview of AWS Systems Manager and the process of setting up AWS Systems Manager, and focuses on the services within the operations management category.

Learning Objectives:

- Define systems management on AWS.
- Describe an application developer's role in systems management.
- Explain the categories of systems management on AWS.
- Identify the AWS tools and services available tor AWS systems management.
- Identify how AWS Systems Manager capabilities align with categories of systems management on AWS.
- Explain how to set up Systems Manager for Amazon EC2 instances with a general setup and a quick setup.
- Create an SSM document that could be used to deploy infrastructure changes through scripting.
- Identify the capabilities of AWS Systems Manager used for operations management and ideal use cases.

Module Outline:

1. **Systems Management**
   a. Introduction: Systems Management
   b. Systems Management on AWS
   c. Knowledge Check
2. **Setting Up AWS Systems Manager**

   a. Introduction: Setting Up AWS Systems Manager
   b. Setup for AWS Systems Manager
   c. SSM Agent
   d. Quick Setup
   e. Lab: Introduction to AWS Systems Manager Documents
   f. Knowledge Check

3. **Operations Management**
   a. Introduction: Operations Management
   b. Operations Management on AWS
   c. AWS Systems Manager Incident Manager
   d. AWS Systems Manager OpsCenter
   e. AWS Systems Manager Explorer
   f. Amazon CloudWatch Dashboards Hosted by Systems Manager
   g. Knowledge Check

Hands-on Labs:

- **Lab: Introduction to AWS Systems Manager Documents (60 min)**
  - In this lab, you explore AWS Systems Manager documents (SSM documents). An SSM document defines the actions that Systems Manager performs on your managed instances. Systems Manager includes more than 100 pre-configured documents that you can use by specifying parameters at runtime. You also deploy an SSM document to install a web server on an Amazon EC2 instance.

Week 6: Systems Management – Part 2

Goal:

Gain System Management knowledge and skills in key topics related to node management, such as Fleet Manager, Compliance, Inventory, Session Manager, Run Command, State Manager, Patch Manager, and Distributor.

Learning Objectives:

- Define application management on AWS.
- Identify the capabilities of AWS Systems Manager used for application management, and their benefits.
- Describe the use cases for each capability.
- Explain the functionality and benefits of Parameter Store.
- Define change management for AWS Systems Manager.
- Identify the Systems Manager capabilities for change management and their benefits.
- Describe a use case for each change management capability of Systems Manager.
- Define node management on AWS.
- Identify the capabilities of AWS Systems Manager used for node management and their benefits.
- Describe a use case for each capability.

Module Outline:

1. **Application Management**

   a. Introduction: Application Management
   b. Application Manager
   c. AWS AppConfig
   d. Parameter Store
   e. Lab: Create a Systems Manager Parameter
   f. Knowledge Check

2. **Change Management**
   a. Introduction: Change Management
   b. Change Manager
   c. Automation
   d. Lab: Resize Amazon EC2 Instances with Automation
   e. Change Calendar
   f. Maintenance Windows
   g. Knowledge Check
3. **Node Management**
   a. Introduction: Node Management
   b. Node Management on AWS
   c. State Manager
   d. Session Manager
   e. Run Command
   f. AWS Systems Manager Distributor
   g. Lab: Create a Package in Systems Manager Distributor
   h. Knowledge Check

Activities:

- **Lab: Create a Systems Manager Parameter (60 min)**
  - Parameter Store provides a means to manage configuration data and secrets for your applications. Recall that decoupling your application's configuration from the source code is a common best practice. Managing your application's configuration and secrets with Parameter Store parameters follows that best practice. For this lab, you will use Parameter Store to launch an Amazon EC2 instance.
- **Lab: Resize Amazon EC2 Instances with Automation (30 min)**
  - Deploying changes manually to a fleet of Amazon EC2 instances is time-intensive and includes a high risk of errors. To save time and reduce errors, automating the deployment of changes to Amazon EC2 instances is a preferred method. For this lab, you practice automating changes to Amazon EC2 instances using Automation, a capability of AWS Systems Manager.
- **Lab: Create a Package in Systems Manager Distributor (30 min)**
  - In this lab, you use Distributor, a capability of AWS Systems Manager, to create the Amazon CloudWatch agent custom package. You will then use Run Command to install this package.

Week 7: Scripting – Part 1

Goal:

Gain foundational knowledge of the key aspects of scripting, including an introduction to scripting, an overview of AWS CLI, scripting with the Bash Shell language, and a brief overview of error handling/troubleshooting using Bash Shell.

Learning Objectives:

- Define and explain applications of scripting.
- Describe the key characteristics of scripting languages.
- Explain synchronous and asynchronous processing.
- Discuss AWS CLI characteristics, purpose, and basic examples.
- Discuss use cases and benefits of using AWS CloudShell.
- Use CloudShell to interact with AWS resources.
- Define the Bash shell.
- Discuss and define variables and loops.
- Discuss and define conditionals and functions.
- Discuss trap and exit.
- Discuss graceful degradation.
- Discuss retries and exponential backoff.
- Discuss logging techniques.

Module Outline:

1. **Getting Started with Scripting**
    a. Introduction: Getting Started with Scripting
    b. Introduction to Scripting
    c. Overview of Scripting Languages
    d. Synchronous and Asynchronous Processing
    e. Knowledge Check
2. **Overview of AWS Command Line Interface (AWS CLI)**
    a. Introduction: Overview of AWS CLI
    b. AWS CLI Basics
    c. Introduction to AWS CloudShell
    d. Demo: Getting Started with AWS CloudShell
    e. Demo: Editing a File with GNU Nano
    f. Lab: Using the AWS CLI in Bash to Interact with AWS
    g. Knowledge Check
3. **Scripting with the Bash Shell**
    a. Introduction: Scripting with the Bash Shell
    b. Bash Shell Overview
    c. Practice Environment: Using Bash
    d. Getting Started with Bash
    e. Bash Fundamentals
    f. Functions
    g. Conditionals

   h. Loops
   i. Bringing It All Together
   j. Lab: Using the AWS CLI and Bash to Automate Linux
   k. Knowledge Check

4. **Error Handling and Troubleshooting**
   a. Introduction: Error Handling and Troubleshooting
   b. Troubleshooting Overview
   c. Error Handling in Bash
   d. Trap and Exit
   e. Retries and Backoff
   f. Logging
   g. Lab: Troubleshooting AWS CLI and Bash in Linux Environments
   h. Knowledge Check

Hands-on Labs:

- **Lab: Using the AWS CLI in Bash to Interact with AWS (60 min)**
  - In this lab, you run commands in a Linux environment running on an Amazon EC2 instance. You create and navigate through directories and files, and you use AWS CLI to create AWS services.
- **Lab: Using the AWS CLI and Bash to Automate Linux (60 min)**
  - In this lab, you run commands in the Linux environment running on an Amazon EC2 instance. You create and navigate through directories and files, and you use AWS CLI to create AWS services.
- **Lab: Troubleshooting AWS CLI and Bash in Linux Environments (60 min)**
  - In this lab, you troubleshoot the upload.sh script to find the issues with the Amazon S3 bucket setup, and the backup.sh script to find issues with Linux file permissions and implement retry logic in the upload.sh script.

Week 8: Scripting – Part 2

Goal:

Gain a foundational knowledge key aspects of scripting, including an overview of AWS Tools for PowerShell, scripting with the PowerShell language, and error handling/troubleshooting with PowerShell.

Learning Objectives:

- Discuss AWS Tools for PowerShell characteristics and purpose.
- Explain AWS Tools for PowerShell features.
- Describe how to install, set up, and use AWS Tools for PowerShell.
- Discuss and define variables.
- Discuss basic syntax of PowerShell scripting.
- Discuss and define loops and conditionals.
- Discuss, define, and identify functions and parameters.
- Discuss basic error checks and conditional execution in PowerShell.
- Discuss and provide examples of trap and exit in PowerShell.
- Discuss retries and backoff in PowerShell.

Module Outline:

1. **Overview of AWS Tools for PowerShell**
    a. Introduction: Overview of AWS Tools for PowerShell
    b. Overview of AWS Tools for PowerShell
    c. Key Features of AWS Tools for PowerShell
    d. Demo: AWS Tools for PowerShell
    e. Lab: Using the AWS CLI in Windows to Interact With AWS
    f. Knowledge Check
2. **Scripting with PowerShell**
    a. Introduction: Scripting with PowerShell
    b. Practice Environment: Using PowerShell
    c. Getting Started with PowerShell
    d. PowerShell Fundamentals
    e. Loops
    f. Conditional Statements
    g. Demo: Scripting with PowerShell
    h. Lab: Using the AWS Tools for Windows PowerShell to Automate Windows
    i. Knowledge Check
3. **Error Handling and Troubleshooting with PowerShell**
    a. Introduction: Error Handling and Troubleshooting with PowerShell
    b. Error Handling in PowerShell
    c. Exception Handling Statements
    d. Retries and Backoff
    e. Logging
    f. Lab: Troubleshooting the AWS Tools for Windows PowerShell in Windows Environments
    g. Knowledge Check

Hands-on Labs:

- **Lab: Using the AWS CLI in Windows to Interact with AWS (60 min)**
    - In this lab, you run commands in the Windows environment running on an Amazon EC2 instance. You create and navigate through directories and files and use the AWS Command Line Interface (AWS CLI) to create AWS services.
- **Lab: Using the AWS Tools for Windows PowerShell to Automate Windows (60 min)**
    - In this lab, you navigate a Windows environment to inspect an existing application, create and modify folders and files for your maintenance solution, create Windows PowerShell scripts to take backups and upload files to the AWS Cloud, and schedule the maintenance scripts to run automatically.
- **Lab: Troubleshooting the AWS Tools for Windows PowerShell in Windows Environments (60 min)**
    - In this lab, you will inspect the kiosk environment to make sure that it has been set up properly, review the log output to troubleshoot Windows PowerShell scripts, and implement retry logic in a Windows PowerShell script using a loop.

Week 9: DevOps 1 – Part 1

Goal:

Gain a foundational knowledge of the principles and methodologies of DevOps, version control, and code repositories.

Learning Objectives:

- Describe how DevOps works and its benefits.
- Discuss key principles and methodologies of DevOps.
- Identify and discuss various DevOps tools used by a developer.
- Identify common code repositories.
- Define version control and identify different types of version control services.
- Discuss the benefits of version control.
- Explore AWS CodeCommit.

Module Outline:

1. **Getting Started with DevOps**
    a. Introduction: Getting Started with DevOps
    b. Welcome to the DevOps 1 Module
    c. DevOps Overview
    d. Benefits of DevOps
    e. Roles in DevOps
    f. DevOps Best Practices
    g. AWS Services and Tools for Different Practices
    h. Knowledge Check
2. **Understanding Code Repositories**
    a. Introduction: Understanding Code Repositories
    b. Overview of Version Control Systems
    c. Types of Version Control Systems
    d. Code Repositories
    e. Introduction to AWS CodeCommit
    f. Lab: Working with AWS CodeCommit
    g. Knowledge Check

Hands-on Labs:

- **Lab: Working with AWS CodeCommit (45 min)**
    - In this lab, you first create a code repository in AWS CodeCommit. Then you create a local repository on a Linux instance running in Amazon EC2. After you create the local repo, you make changes to it and synchronize (commit) your changes to the CodeCommit repository.

Week 10: DevOps 1 – Part 2

Goal:

Gain a foundational knowledge about the basics of GIT with commands and automation using continuous integration and continuous delivery (CI/CD).

Learning Objectives:

- Pull codebase from Git into AWS CodeCommit.
- Push code base from AWS CodeCommit to Git.
- Identify how to create and checkout a branch of an AWS CodeCommit repository.
- Provide an overview of CI/CD.
- Outline various CI/CD paradigms.
- Describe the function of common source, build, and deployment tools.
- Describe common pipeline tools.
- Provide a summary of automation.

Module Outline:

1. **Transferring Code from One Repository to the Other**
    a. Introduction: Transferring Code from One Repository to the Other
    b. Working with Code Repositories
    c. Pulling and Pushing Code
    d. Using Branching
    e. Knowledge Check
2. **Using Automation Tools to Design a Pipeline**
    a. Introduction: Using Automation Tools to Design a Pipeline
    b. Introduction to CI/CD
    c. Setting Up a CI/CD Pipeline with AWS Developer Tools
    d. Pipeline Examples
    e. Lab: Introduction to AWS CodeDeploy
    f. Knowledge Check

Hands-on Labs:

- **Lab: Introduction to AWS CodeDeploy (45 min)**
    - In this lab, you deploy a sample service application to two Amazon EC2 instances that have already been configured through the lab template. Use AWS CodeDeploy to push software onto a fleet of Amazon EC2 instances and have the software automatically deployed, registered, and started.

Week 11: DevOps 1 – Part 3

Goal:

Gain a foundational knowledge of infrastructure as code (IaC), AWS CloudFormation, AWS Cloud Development Kit (AWS CDK), development best practices, and testing strategies.

Learning Objectives:

- Identify examples of AWS CloudFormation templates.
- Modify a CloudFormation template and create a stack.
- Describe the benefits of AWS CDK.
- Describe the usage of multiple environment stages and the benefits of a consistent environment for application builds.
- Identify the branching model trunk-based development.
- Outline and describe the benefits of implementing critical testing practices early in development.
- Identify developer collaboration on code review and pull requests.
- Describe developer tasks for automated testing in continuous integration.

Module Outline:

1. **Understanding IaC**
   a. Introduction: Understanding IaC
   b. Introduction to IaC
   c. CloudFormation Overview
   d. Lab: Using AWS CloudFormation
   e. Introduction to AWS CDK
   f. Lab: Configuring the AWS CDK Credentials
   g. Knowledge Check
2. **Software Development Practices**
   a. Introduction: Software Development Practices
   b. Environments in Software Development
   c. Automated Testing
   d. Unit Testing
   e. Shift-Left Approach to Software Testing
   f. Using a Trunk-Based Workflow
   g. AWS CodeCommit Pull Requests
   h. Knowledge Check

Hands-on Labs:

- **Lab: Using AWS CloudFormation (45 min)**
  - In this lab, you will create an environment for a development team. The development team has asked for an Apache web server with HTTP access. The requirements document asks for a dedicated virtual private cloud (VPC), a single public subnet, and a small Amazon EC2 instance. You use your AWS Cloud9 environment to modify an existing CloudFormation template to meet the requirements of the development team. You modify the template to use the CloudFormation change set, and detect drift functionality.
- **Lab: Configuring the AWS CDK Credentials (45 min)**
  - In this lab, you create a virtual private cloud (VPC) and add an Amazon EC2 instance with AWS Systems Manager enabled using AWS Cloud Development Kit (AWS CDK).