AWS Cloud Institute: Cloud Operations 2 Syllabus

Course Overview

In this course, you will have the opportunity to practice with application deployment services and strategies, learn how to enable DevOps teams, and understand Infrastructure as Code (IaC) and its benefits. This course introduces you to the AWS Cloud Development Kit (CDK) and guides you through setting up an environment to work with AWS CDK in Python. You will also develop functional knowledge of distributed tracing and troubleshooting with Amazon X-Ray, and understand open-source monitoring. Lastly, you will be able to discuss application troubleshooting with Amazon CloudWatch.

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

Cloud Operations 1

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: DevOps 2 – Part 1

Goal:

Build your knowledge of continuous Integration and Continuous Delivery (CI/CD) by exploring its significance and best practices. Learn how to automate testing processes with Continuous Integration and AWS CodeBuild to ensure efficient and reliable software delivery pipelines. Gain insight into integrating code reviews into automated testing workflows to foster collaboration and code quality.

Learning Objectives:

- Define and explain the core principles of CI/CD.
- Describe the benefits and challenges of implementing CI/CD.
- Identify the key components of a CI/CD pipeline.
- Explain best practices for a CI/CD pipeline.
- Explain the benefits of automating testing code changes.
- Describe code coverage and its purpose for code testing.

- Identify non-AWS testing code tools.
- Describe how AWS CodeBuild performs application testing.
- State the types of testing AWS CodeBuild can perform.
- Configure AWS CodeBuild to perform application testing.
- Describe the relationship between automated testing and code reviews.
- Explore techniques for automated testing and code review integration.
- Explain what Amazon CodeGuru is, its benefits, and use cases.
- Understand how CodeGuru helps with manual code reviews

Module Outline:

1. **Review of Continuous Integration and Continuous Delivery (CI/CD)**
    a. Introduction: Review of CI/CD
    b. Review of DevOps Principles
    c. CI/CD Core Principles
    d. Benefits and Challenges of CI/CD
    e. Best Practices for CI/CD Pipelines
    f. Knowledge Check
2. **Automate Testing with Continuous Integration**
    a. Introduction: Automate Testing with Continuous Integration
    b. Testing Code Changes
    c. Unit Testing in CI/CD
    d. Benefits of Automating Testing Code Changes
    e. Code Coverage and its Purpose for Code Testing
    f. Non-AWS Unit Testing Code Tools
3. **Automate Testing with AWS CodeBuild**
    a. Introduction: Automate Testing with AWS CodeBuild
    b. Review of AWS CodeBuild
    c. Types of Testing in AWS CodeBuild
    d. Lab: Using AWS CodePipeline for Unit Testing
    e. Knowledge Check
4. **Integrating Code Reviews in Automated Testing**
    a. Introduction: Integrating Code Reviews in Automated Testing
    b. Automated Testing and Code Reviews
    c. Methods for Automated Testing and Code Review Integration
    d. Amazon CodeGuru
    e. Lab: Automating Code Reviews with Amazon CodeGuru
    f. Knowledge Check

Hands-on Labs:

- **Lab: Using AWS Code Pipeline for Unit Testing (60 min)**
    - This lab demonstrates how to use AWS CodePipeline to perform unit testing for an application.
- **Lab: Automating Code Reviews with Amazon CodeGuru (60 min)**
    - In this lab, you will use CodeGuru to perform a review on existing code.
- **AWS SimuLearn Challenge: CI/CD Pipelines for APIs (60 min)**

- In this lab, you have been assigned the vital task of repairing and finalizing the CI/CD pipeline for the company's APIs. While the core architecture is already in place, some key configurations are missing. Your goal is to complete the required tests and make sure the pipeline is fully operational. When your task is successfully completed, the Task Manager application will be fully functional, so employees can create and manage tasks efficiently.

Week 2: DevOps 2 – Part 2

Goal:

Learn about the CI/CD pipeline and how it enables seamless automated software delivery. You will also explore various deployment strategies for continuous delivery and deployment to ensure efficient and reliable releases. You will also learn how to provide consistent and dependable DevOps environments to enable streamlined development and operations processes.

Learning Objectives:

- Explain an application developer's role and responsibilities with continuous delivery.
- Explain how AWS CodePipeline works and its benefits.
- Describe AWS CodeDeploy and its benefits and purpose.
- Explain CodeDeploy components.
- Explain the need for a deployment strategy in continuous delivery and deployment.
- Describe various deployment strategies.
- Evaluate application deployment requirements.
- Recommend an appropriate deployment strategy.
- Describe the need for managing DevOps standardization.
- Explain the requirements of DevOps standardization tools.
- Describe AWS Proton, its purpose, and the benefits.
- Create services and environments with AWS Proton.
- Explain how AWS Service Catalog provides a self-service experience.

Module Outline:

1. **Integrating with the CI/CD Pipeline**
    a. Introduction: Integrating with the CI/CD Pipeline
    b. The Application Developer Role in CI/CD
    c. Continuous Delivery Pipeline Requirements
    d. Review of AWS CodeDeploy
    e. Review of AWS CodePipeline
    f. Code Testing in Continuous Delivery
    g. Lab: Using AWS CodePipeline for Integration Testing
    h. Knowledge Check
2. **Deployment Strategies for Continuous Delivery and Deployment**
    a. Introduction: Deployment Strategies
    b. Types of Deployment Strategies for CD

   c. In-Place Deployments
   d. Immutable Updates
   e. Rolling Deployments
   f. Blue/Green Deployments
   g. Lab: Blue/Green Deployments with AWS CodeDeploy and Amazon EC2
   h. Knowledge Check
3. **Providing Reliable and Consistent DevOps Environments**
   a. Introduction: Providing Reliable and Consistent DevOps Environments
   b. Managing DevOps Standards
   c. AWS Proton
   d. Demo: Creating Environments and Services with AWS Proton
   e. AWS Service Catalog
   f. Demo: Create Deployment Pipeline with AWS Service Catalog
   g. Lab: Deploying Standardized Assets Using AWS Service Catalog
   h. Knowledge Check

Hands-on Labs:

- **Lab: Using AWS CodePipeline for Integration Testing (60 min)**
  - This lab focuses on integrating automated integration testing into a Continuous Integration and Continuous Delivery (CI/CD) pipeline using CodePipeline. You gain hands-on experience in configuring the pipeline to include an integration testing stage, which validates the application's functionality before deployment.
- **Lab: Blue/Green Deployments with AWS CodeDeploy and Amazon EC2 (90 min)**
  - In this lab, you set up a blue-green deployment strategy using CodeDeploy for an existing CodeCommit repository and CodePipeline deployment. You learn to create a new deployment group, add an application load balancer, and modify the existing deployment to perform blue-green deployments across the two Amazon EC2 instances.
- **Lab: Deploying Standardized Assets Using AWS Service Catalog (90 min)**
  - In this lab, you create an AWS Service Catalog portfolio that contains four products. Each AWS Service Catalog product is backed by an AWS CloudFormation template, which is supplied as part of the lab.

Week 3: DevOps 2 – Part 3

Goal:

Explore the concept of development, security, and operations (DevSecOps) to understand its significance in integrating security practices throughout the software development lifecycle. You will also learn about practical approaches to applying DevSecOps principles.

Learning Objectives:

- Describe DevSecOps and its role in securing software delivery.
- Identify DevSecOps components.
- Identify common vulnerabilities in software development.
- Explain common security testing practices in software development.

- Identify AWS and third-party security testing tools.
- Explain the role of CodeGuru Security in security testing.
- Explain how Amazon Inspector automates vulnerability management at scale.
- Explain DevSecOps best practices.

Module Outline:

1. **DevSecOps**
    a. Introduction: DevSecOps
    b. The Role of DevSecOps
    c. Key Components of DevSecOps
    d. Common Vulnerabilities in Software Development
    e. Security Testing Practices in DevSecOps
    f. Security Testing Practices in DevSecOps
    g. Demo: SAST
    h. Knowledge Check
2. **Applying DevSecOps**
    a. Introduction: Applying DevSecOps
    b. Security Testing Tools
    c. Getting Started with Amazon CodeGuru Security
    d. Getting Started with Amazon Inspector
    e. Scenario: DevSecOps Best Practices
    f. Lab: Vulnerability Scanning with Amazon Inspector
    g. Knowledge Check

Hands-on Labs:

- **Lab: Using Amazon Inspector for Vulnerability Scanning (75 min)**
    - In this lab, you will use Amazon Inspector to scan for vulnerabilities in your AWS resources, specifically Amazon EC2 instances and AWS Lambda functions. You learn how to configure Amazon Inspector, interpret the vulnerability reports, and remediate the findings.
- **AWS SimuLearn Lab: Secure Self-Service Infrastructure (60 min)**
    - In this lab, you will help the new head of the IT Services department at a web gaming company who has limited staff to deploy IT services to other departments. The IT Services department is looking for a way to hand off these deployments to the other departments themselves, something like a self-service tool in which configurations already meet compliance requirements and resources are secure.
- **AWS SimuLearn Lab: Securing Your Servers (60 min)**
    - In this lab, you will help a mining operation which built an enterprise resource planning (ERP) application to process job applicant submissions. The application is deployed and running, but the mining operation wants help setting least privilege permissions to limit the application's effect on AWS resources.

Week 4: Infrastructure as Code – Part 1

Goal:

Build on what you learned in DevOps 1 about infrastructure as code (IaC) and how it fits into a DevOps workflow. Discover both AWS and Non-AWS IaC tools, such as AWS CloudFormation, AWS CDK, and Terraform.

Learning Objectives:

- Define IaC and its benefits.
- Describe the problems IaC solves in traditional infrastructure management.
- Identify the benefits of IaC for application developers in a DevOps environment.
- Explain how IaC fits into the DevOps workflow.
- Identify an application developer's responsibilities in writing and maintaining IaC templates.
- Describe how application developers and infrastructure teams work together over IaC.
- Explain the common components and requirements of an IaC tool.
- Describe both AWS and non-AWS IaC tools.
- Describe Rules in CloudFormation and discuss working with them.
- Explain Intrinsic functions in CloudFormation and discuss working with them.
- Describe Conditions in CloudFormation and discuss working with them.
- Define the *DependsOn* attribute and describe its use.
- Define Template Macros and describe how they work.
- Describe the benefits of modules and explain how they work.
- Explain using the CloudFormation Designer.

Module Outline:

1. **Review Infrastructure as Code**
    a. Introduction: Review of Infrastructure as Code
    b. Define Infrastructure as code
    c. Knowledge Check
2. **IAC as a Part of a DevOps Workflow**
    a. Introduction: IaC as a Part of a DevOps Workflow
    b. Deploying Infrastructure as Code with AWS CodePipeline
    c. Developer Responsibilities in Writing and Maintaining IaC Templates
    d. How Developers and Infrastructure Teams Work Together over IaC
    e. Knowledge Check
3. **IaC Tools**
    a. Introduction: IaC Tools
    b. Common Components and Requirements of an IaC Tool
    c. AWS and Third-Party IaC Tools
    d. Building a Serverless Application with AWS Application Composer
    e. Knowledge Check
4. **Building Templates in AWS CloudFormaton**
    a. Introduction: Building Templates in AWS CloudFormaton
    b. Review of AWS CloudFormation
    c. AWS CloudFormation Templates
    d. Leveraging CloudFormation Utilities
    e. Knowledge Check

Hands-on Labs:

- **Lab: Deploying Infrastructure as Code with AWS CodePipeline (60 mins)**
  - In this lab, you will use CodePipeline to deploy infrastructure as code (IaC) using an AWS CloudFormation template. This lab includes steps for building out a CloudFormation template, creating a CodePipeline by pulling source code from CodeCommit, and finally, creating and updating a CloudFormation stack.
- **Lab: Deploying Infrastructure as Code with AWS CodePipeline (60 mins)**
  - In this lab, you will gain hands-on experience using AWS Application Composer by creating a serverless application
- **Lab: Leveraging CloudFormation Utilities (60 mins)**
  - In this lab, you will work with an existing AWS CloudFormation template that has been stripped of its intrinsic functions, conditions, and rules. The template includes comments and instructions guiding you on how to complete the missing elements. By filling in the necessary CloudFormation utilities, you will develop your understanding of these advanced features.

Week 5: Infrastructure as Code – Part 2

Goal:

Learn how to build in AWS CloudFormation, work with CloudFormation stacks, explore CloudFormation Registry, use the AWS Cloud Development Kit, and test CDK constructs.

Learning Objectives:

- Define a stack and change set.
- List stack failure options in CloudFormation.
- Identify the types of resources that support drift detection.
- State the reasons for exporting and importing values from a stack.
- Explain nested Stacks.
- State ways of working with Windows Stacks.
- Discuss rolling back your infrastructure and the purpose of preparing for failure.

Module Outline:

1. **Working with AWS CloudFormation Stacks**
   a. Introduction: Working with AWS CloudFormation Stacks
   b. Building and Managing Stacks
   c. Remediating Stack Drift
   d. Encountering Stack Failures
   e. Deploying Multiple Stacks
   f. Deploying Advanced CloudFormation Stacks
   g. Knowledge Check
2. **Expanding AWS CloudFormation Usage**
   a. Introduction: AWS CloudFormation Usage
   b. Using the CloudFormation Registry
   c. Exploring Amazon EventBridge

   d. Knowledge Check
3. **Examining AWS Cloud Development Kit**
   a. Introduction: Examining AWS Cloud Development Kit
   b. Provisioning Resources with AWS CDK
   c. Working with Constructs in AWS CDK
   d. Knowledge Check
4. **Testing AWS CDK Constructs**
   a. Introduction: Testing AWS CDK Constructs
   b. Testing Methods Used with CDK Apps
   c. Knowledge check

Hands-on Labs:

- **Lab: Deploying Advanced CloudFormation Stacks (60 Mins)**
  - In this lab, learners use CloudFormation to create a nested stack, experience provisioning failure with stack failure options, and modify a nested stack from a change set.
- **AWS SimuLearn Challenge: Automation with CloudFormation (60 min)**
  - In this lab, you will help reduce human error and standardize a robotics research deployment infrastructure.
- **Lab: Working with Constructs in AWS CDK (60 Mins)**
  - In this lab, learners use AWS CDK within the Cloud9 IDE to deploy and test a Lambda function, and the API Gateway REST API.

Week 6: 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 7: 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.
- **AWS SimuLearn Lab: Highly Available Web Applications (60 min)**
  - In this lab, you will help a travel agency create a highly available web application architecture.

Week 8: Monitoring and Troubleshooting – Part 1

Goal:

Learn the methodology to troubleshoot common technical use cases by using AWS CloudTrail and AWS Identity and Access Management (IAM).

Learning Objectives:

- Explain the importance of a structured troubleshooting methodology and its benefits over ad-hoc troubleshooting approaches.
- Describe the key steps involved in the troubleshooting methodology.
- Apply a troubleshooting methodology to diagnose common issues related to cloud infrastructure.
- Develop a troubleshooting plan for a given cloud application scenario.
- Recall the purpose of AWS CloudTrail and differentiate between event types.
- Analyze CloudTrail log files to identify potential security incidents.
- Integrate CloudTrail with AWS services to automate log management and analysis processes.
- Implement best practices for securing and managing CloudTrail trails.
- Explain the purpose and functionality of CloudTrail Lake.

Module Outline:

1. **Troubleshooting Methodology**
    a. Introduction: Troubleshooting Methodology
    b. Troubleshooting Methodology and Structured Approach
    c. Using Troubleshooting Methodology in Cloud Infrastructure
    d. Developing a Troubleshooting Plan
    e. Knowledge Check
2. **Troubleshooting with AWS CloudTrail**
    a. Introduction: Troubleshooting with AWS CloudTrail
    b. What is AWS CloudTrail
    c. Analyzing AWS CloudTrail Log Files for Potential Security Incidents
    d. AWS CloudTrail Integration
    e. Best Practices for Securing and Managing AWS CloudTrail
    f. AWS CloudTrail Lake
    g. Knowledge Check
3. **Troubleshooting in AWS Identify Access Management (IAM)**
    a. IAM Policies
    b. Troubleshooting Common Errors in IAM Policies
    c. Troubleshooting Issues in IAM Role Assumptions, Trust Relationships, and Service-linked Roles
    d. Tools and Services that Can Be Used To Troubleshoot and Audit IAM
    e. Best Practices for IAM Policy Management
    f. Knowledge Check

Hands-on Labs:

- **Lab: Amazon EC2 Observability – Monitoring and Troubleshooting (75 min)**
    - In this lab, you have an opportunity to explore monitoring tools for your Amazon EC2 workloads, as well as apply troubleshooting steps to correct issues affecting your current workloads.
- **Lab: Performing a basic audit of your AWS Environment (45 min)**
    - In this lab, you perform basic audits of core AWS resources. You use the AWS Management Console to understand how to audit the use of multiple AWS services, such as Amazon EC2, Amazon VPC, Amazon IAM, Amazon Security Groups, AWS CloudTrail, and Amazon CloudWatch.

Week 9: Monitoring and Troubleshooting – Part 2

Goal:

Learn the importance of metric monitoring using Amazon CloudWatch, Lambda Insights, Internet Monitor and Network Monitor.

Learning Objectives:

- Use custom metrics for deeper insights.
- Discuss enabling cross-account, cross-Region monitoring.
- Recall CloudWatch anomaly detection and create a CloudWatch alarm based on anomaly detection.

- Use CloudWatch Metrics Insights to create alarms.
- Recall CloudWatch Container Insights and set up Container Insights on Amazon Elastic Container. Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS).
- Discuss troubleshooting with Container Insights.
- Recall CloudWatch Lambda Insights and use Lambda Insights.
- Identify root cause monitored by Lambda Insights
- Describe CloudWatch Internet Monitor and CloudWatch Network Monitor.

Module Outline:

1. **Metric Monitoring**
    a. Introduction: Metric Monitoring
    b. Custom Metrics
    c. Data Aggregation
    d. Cross-Account Cross-Region Monitoring
    e. Amazon CloudWatch Anomaly Detection
    f. Alarms with Amazon CloudWatch Metrics Insights
    g. Activity: Exploring a Use Case Scenario with Amazon CloudWatch Custom Metrics
    h. Knowledge Check
2. **Insights and Network Monitoring**
    a. Introduction: Insights and Network Monitoring
    b. Using Amazon CloudWatch Container Insights
    c. Troubleshooting with CloudWatch Container Insights
    d. Using Amazon CloudWatch Lambda Insights
    e. Troubleshooting with CloudWatch Lambda Insights
    f. Amazon CloudWatch Internet Monitor
    g. Amazon CloudWatch Network Monitor
    h. Knowledge Check

Hands-on Labs:

- **AWS SimuLearn Lab: Monitor and Analyze Network Traffic (60 min)**
    - In this lab, you will help aerospace engineers who want to monitor and analyze network traffic to detect misuse of a space station's data and systems. The engineers want to capture information about IP traffic going to and from the network interfaces of each system, and then analyze the information to detect unusual network activity.
- **AWS SimuLearn Lab: Traffic Mirroring (60 min)**
    - In this lab, the general of a galactic security fleet needs your help to ensure that their spaceships and planetary bases are secure from any potential threats. The general wants a solution to monitor the fleet's network traffic from their spaceships and bases, and test the network's effectiveness.

Assessments:

For each module, you will complete a series of ungraded assessments to help measure your progress. At the end of each week, you will complete a graded final assessment that tests your knowledge of the learning objectives presented. A passing grade of 85% is required to move forward with your learning, and you can take final assessments as many times as needed.

Week 10: Monitoring and Troubleshooting – Part 3

Goal:

Learn how to implement metric filters and Live Tail for monitoring, use Amazon CloudWatch Logs, discuss Amazon CloudWatch Logs, and discuss troubleshooting with VPC Flow Logs.

Learning Objectives:

- Implement metric filters and Live Tail for monitoring.
- Use Amazon CloudWatch Logs Insights for querying and analyzing log data.
- Discuss Amazon CloudWatch Logs anomaly detection and pattern analysis.
- Discuss troubleshooting with VPC Flow Logs.

Module Outline:

1. **Logs**
    a. Introduction: Logs
    b. Metric Filters
    c. Live Tail Data with CloudWatch Logs
    d. Querying with CloudWatch Log Insights
    e. Log Anomaly Detection and Pattern Analysis
    f. Troubleshooting with VPC Flow Logs
    g. Lab: Monitoring Applications and Infrastructure
    h. Knowledge Check
2. **Application Monitoring**
    a. Introduction: Application Monitoring
    b. Using CloudWatch Application Insights
    c. Using CloudWatch Synthetics
    d. Using CloudWatch RUM
    e. Application Signals
    f. Knowledge Check

Hands-on Labs:

- **Lab: Monitoring applications and Infrastructure (60 Mins)**
    - In this lab, you will practice setting up and monitoring metrics for business-application events, define relevant event thresholds for metrics, create an automated notification, and perform a remediation when metric thresholds are exceeded.

Week 11: Monitoring and Troubleshooting – Part 4

Goal:

Build foundational knowledge about the principles and implementations of distributed tracing with AWS X-Ray.

Learning Objectives:

- Discuss the features, benefits, and concepts of AWS X-Ray.
- Explain traces.
- Explore service graphs.
- Explore trace maps.
- Describe how to use filter expressions.
- Describe cross-account tracing.
- Understand how to use tracing with X-Ray.
- Explain latency histograms.
- Discuss X-Ray insights.
- Describe the X-Ray Analytics console.
- Discuss X-Ray SDK for Python.

Module Outline:

1. **VPC Reachability Analyzer**
    a. Introduction: VPC Reachability Analyzer
    b. Reachability Analyzer Functionality
    c. Reachability Analyzer Use Cases
    d. Troubleshooting with Reachability Analyzer
    e. Lab: Troubleshooting Website Reachability behind a Load Balancer
    f. Knowledge Check
2. **Tracing with AWS X-Ray**
    a. Introduction: Tracing with AWS X-Ray
    b. X-Ray Features and Functionality
    c. X-Ray Concepts
    d. Tracing Demo
    e. Knowledge Check
3. **Troubleshooting and Monitoring with AWS X-Ray**
    a. Introduction: Troubleshooting and Monitoring with AWS X-Ray
    b. Latency Histograms
    c. X-Ray Insights
    d. X-Ray Analytics
    e. X-Ray SDK for Python
    f. Knowledge Check

Hands-on Labs:

- **Lab: Troubleshooting Website Reachability behind a Load Balancer (60 Mins)**
    - In this lab, you will explore the concepts of configuring a web server behind an Elastic Load Balancer (ELB). You will address a scenario where users are not able to reach a website hosted on an Amazon Elastic Compute Cloud (Amazon EC2) instance behind a load balancer.
- **AWS SimuLearn Lab: Core Security Concepts (60 min)**
    - In this lab, you will improve security at the city's stock exchange by ensuring that support engineers can perform only authorized actions.