AWS Certified DevOps Engineer Professional (DOP-C01)

Introduction

The AWS Certified DevOps Engineer - Professional (DOP-CO1) examination validates technical expertise in provisioning, operating, and managing distributed application systems on the AWS platform. It is intended for individuals who perform a devops engineer role.

It validates an examinee's ability to:

- Implement and manage continuous delivery systems and methodologies on AWS.
- Implement and automate security controls, governance processes, and compliance validation.
- Define and deploy monitoring, metrics, and logging systems on AWS.
- Implement systems that are highly available, scalable, and self-healing on the AWS platform.
- Design, manage and maintain tools to automate operational processes.

Course Objective

This course teaches you about core aspects such as:

- Managing and Implementing continuous delivery systems and methodologies on AWS
- Automating governance processes, security controls, and compliance validation
- Monitoring metrics, and logging systems on AWS
- Implementing systems that are highly scalable, and self-replicator on the AWS platform
- Designing, managing, and maintaining tools and services to automate operational processes

Course Outline

Domain 1: SDLC Automation

1.1 Apply concepts required to automate a CI/CD pipeline
1.2 Determine source control strategies and how to implement them
1.3 Apply concepts required to automate and integrate testing
1.4 Apply concepts required to build and manage artifacts securely
1.5 Determine deployment/delivery strategies (e.g., A/B, Blue/green, Canary, Red/black) and how to implement them using AWS Services

Domain 2: Configuration Management and Infrastructure as Code

2.1 Determine deployment services based on deployment needs
2.2 Determine application and infrastructure deployment models based on business needs
2.3 Apply security concepts in the automation of resource provisioning
2.4 Determine how to implement lifecycle hooks on a deployment
2.5 Apply concepts required to manage systems using AWS configuration management tools and services

Domain 3: Monitoring and Logging

3.1 Determine how to set up the aggregation, storage, and analysis of logs and metrics
3.2 Apply concepts required to automate monitoring and event management of an environment
3.3 Apply concepts required to audit, log, and monitor operating systems, infrastructures, and applications
3.4 Determine how to implement tagging and other metadata strategies

Domain 4: Policies and Standards Automation

4.1 Apply concepts required to enforce standards for logging, metrics, monitoring, testing, and security
4.2 Determine how to optimize cost through automation
4.3 Apply concepts required to implement governance strategies

Domain 5: Incident and Event Response

5.1 Troubleshoot issues and determine how to restore operations
5.2 Determine how to automate event management and alerting
5.3 Apply concepts required to implement automated healing
5.4 Apply concepts required to set up event-driven automated actions

Domain 6: High Availability, Fault Tolerance, and Disaster Recovery

6.1 Determine appropriate use of multi-AZ versus multi-region architectures
6.2 Determine how to implement high availability, scalability, and fault tolerance
6.3 Determine the right services based on business needs (e.g., RTO/RPO, cost)
6.4 Determine how to design and automate disaster recovery strategies
6.5 Evaluate a deployment for points of failure

Prerequisites

- Systems Operations on AWS or Developing on AWS
- Working knowledge of one or more high-level programming languages, such as C#, Java, PHP, Ruby, or Python
- Intermediate knowledge of administering Linux or Windows systems at the command-line level
- Working experience with AWS using both the AWS Management Console and the AWS Command Line Interface (AWS CLI)

Target Audience

- System administrators
- Software developers

Duration

- 24 Hours Training Course