INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert
instruction from anywhere.

AWS Certified DevOps Engineer - Professional Boot Camp

The DevOps Engineering on AWS course is designed for the use of DevOps practices and tools to increase your ability to develop and maintain applications at high velocity on AWS with hands-on exercises to help you learn by doing.

Course description

This 3-day Boot Camp is focused on teaching you technical expertise in provisioning, operating, and managing distributed systems and services on AWS in the areas of software development lifecycle (SDLC) concepts, Infrastructure as Code (IaC) options, replication and failover methods, monitoring of applications and infrastructure, event-driven architectures and more.

This boot camp not only teaches you the knowledge and skills of the DevOps engineering it also prepares you to successfully pass the challenging AWS Certified DevOps Engineer - Professional exam.

This course offers enrollment with a voucher. The voucher is pre-paid access to sit for the certifying exam upon eligibility.

Who should attend

- DevOps engineers
- DevOps architects
- Operations engineers
- System administrators
- Developers

Boot camp at a glance

What you'll learn

- ✓ Design and implement an infrastructure on AWS
- ✓ Host secure, highly scalable, and private Git repositories
- ✓ Build CI/CD pipelines to deploy applications on Amazon EC2

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 3-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to hundreds of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with hundreds of additional training courses.

What's included

» Three days of expert, live AWS instruction
» Exam Pass Guarantee
» Exam voucher
» Unlimited practice exam attempts
» 100% Satisfaction Guarantee
» Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and lab)
» 90-day extended access to Boot Camp components, including class recordings
» Knowledge Transfer Guarantee

Prerequisites

None, but prior to enrolling in Infosec's Boot Camp, it is recommended that you have completed the Systems Operations on AWS or Developing on AWS courses and possess a working knowledge of one or more high-level programing languages, such as C#, Java, PHP, Ruby, Python.

Exam objectives

This boot camp prepares you to pass AWS Certified DevOps Engineer - Professional (DOP-C02) exam, which covers 6 domain areas designed to ensure relevancy across all disciplines of information security.

- Domain 1: SDLC Automation
- Domain 2: Configuration Management and IaC
- Domain 3: Resilient Cloud Solutions
- Domain 4: Monitoring and Logging
- Domain 5: Incident and Event Response
- Domain 6: Security and Compliance

Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

DevOps Engineering on AWS details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3
Morning session	Course Introduction Intro to (DOP-C02) Domain 1: SDLC Automation	Domain 3: Resilient Cloud Solutions	Domain 5: Incident and Event Response Domain 6: Security and Compliance
Afternoon session	Domain 2: Configuration Management and IaC	Domain 4: Monitoring and Logging Domain 5: Incident and Event Response	Recap & Review Exam Tips & Practice Exam

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

SDLC Automation

- Repository Management: Configuring repositories for code, images, and artifacts.
- Integration with Version Control: Using version control to connect development pipelines with application environments.
- Build Processes: Establishing build processes, such as AWS CodeBuild.
- Secrets Handling: Managing secrets used in the build and deployment process with tools like AWS Secrets Manager and AWS Systems Manager Parameter Store.
- Deployment Strategies: Determining appropriate deployment strategies, including AWS CodeDeploy.
- Build and Test Automation: Running builds and tests automatically during pull requests or code merges, with services like AWS CodeCommit and CodeBuild.
- Performance Testing: Conducting load/stress tests, performance benchmarking, and large-scale application testing.
- Application Health Measurement: Assessing application health based on exit codes.
- Test Automation: Automating unit tests and code coverage assessments.
- Service Testing: Invoking AWS services within a pipeline for testing.
- Artifact Repository Setup: Creating and configuring artifact repositories using services like AWS CodeArtifact, Amazon S3, and Amazon ECR.
- Artifact Generation Tools: Configuring build tools to generate artifacts, including CodeBuild and AWS Lambda.
- Instance and Image Automation: Automating the creation of Amazon EC2 instances and container images, for instance, with EC2 Image Builder.
- Security Permissions: Configuring security permissions to enable access to artifact repositories, involving AWS IAM and CodeArtifact.
- Deployment Agent Configuration: Configuring deployment agents like the CodeDeploy agent.
- Troubleshooting: Diagnosing and resolving

deployment issues.

- Deployment Methods: Using various deployment strategies such as blue/green and canary deployments.

Configuration Management and IaC

- IaC Template Management: Creating and deploying Infrastructure as Code (IaC) templates, for example, AWS Serverless Application Model (AWS SAM), AWS CloudFormation, and AWS Cloud Development Kit (AWS CDK).
- Cross-Account Deployment: Applying CloudFormation StackSets across multiple AWS accounts and regions.
- Configuration Management Choices: Identifying the most suitable configuration management services, such as AWS OpsWorks, AWS Systems Manager, AWS Config, and AWS AppConfig.
- IaC Integration: Embedding infrastructure patterns, governance controls, and security standards into reusable IaC templates, like AWS Service Catalog, CloudFormation modules, and AWS CDK.
- Account Standardization: Establishing standardized and automated account provisioning and configuration.
- Account Management: Creating, consolidating, and centrally managing accounts using AWS Organizations and AWS Control Tower.
- IAM Solutions: Applying Identity and Access Management (IAM) solutions for complex multi-account and organizational structures, including SCPs and role assumptions.
- Governance and Security: Implementing and developing governance and security controls at scale using AWS Config, AWS Control Tower, AWS Security Hub, Amazon Detective, Amazon GuardDuty, AWS Service Catalog, and SCPs.
- System Automation: Automating system inventory, configuration, and patch management with tools like Systems Manager and AWS Config.
- Lambda Function Development: Creating Lambda function automations for complex scenarios using AWS SDKs, Lambda, and AWS Step Functions.
- Software Configuration: Automating the configuration of software applications to ensure they match the desired state, for instance, with OpsWorks and Systems Manager State Manager.
- Software Compliance: Maintaining software compliance, typically through Systems Manager.

Resilient Cloud Solutions

- Business Resiliency: Converting business requirements into technical resilience needs.
- Fault Remediation: Identifying and addressing single points of failure in current workloads.
- Cross-Region Solutions: Implementing cross-Region solutions using services like Amazon DynamoDB, Amazon RDS, and others.
- Load Balancing: Configuring load balancing to support services across Availability Zones.
- Multi-AZ and Multi-Region Support: Setting up applications and services to function across multiple Availability Zones and Regions while minimizing downtime.
- Scalability Management: Identifying and solving scaling issues.
- Scaling Solutions: Implementing auto-scaling, load balancing, and caching solutions as needed.
- Containerized Apps: Deploying container-based applications with Amazon ECS and EKS.
- Global Scalability: Deploying workloads in multiple Regions for global scalability.
- Serverless Configurations: Configuring serverless applications using services like Amazon API Gateway, Lambda, and AWS Fargate.
- Failover Testing: Testing failover of Multi-AZ and multi-Region workloads for services like Amazon RDS, Aurora, Route 53, and CloudFront.
- Backup Strategies: Identifying and implementing cross-Region backup and recovery strategies using AWS Backup, Amazon S3, and Systems Manager.
- Load Balancer Recovery: Configuring load

balancers for recovery from backend failure.

Monitoring and Logging

- Log Management: Securely storing and managing logs.
- Metrics from Logs: Creating CloudWatch metrics from log events with metric filters.
- Custom Metrics: Collecting custom metrics, for example, through the CloudWatch agent.
- Log Data Processing: Processing log data with CloudWatch log subscriptions, like Kinesis, Lambda, and Amazon OpenSearch Service.
- Search and Analysis: Searching and analyzing log data using filter and pattern syntax or CloudWatch Logs Insights.
- Data Encryption: Configuring encryption for log data with AWS KMS.
- Dashboards and Alarms: Building CloudWatch dashboards and visualizations with Amazon QuickSight and associating alarms with metrics.
- X-Ray Integration: Configuring AWS X-Ray for various services.
- Real-Time Log Streams: Analyzing real-time log streams, such as Kinesis Data Streams.
- Log Analysis Services: Analyzing logs with AWS services like Amazon Athena and CloudWatch Logs Insights.
- Auto Scaling Solutions: Configuring solutions for auto scaling, such as DynamoDB, EC2 Auto Scaling groups, RDS storage auto scaling, and ECS capacity providers.
- Custom Metrics and Notifications: Creating custom metrics, metric filters, alarms, and notifications with services like Amazon SNS and Lambda.
- Event Processing: Configuring S3 events to process log files and deliver them to another destination, like OpenSearch Service and CloudWatch Logs.
- Event Notifications: Setting up EventBridge to send notifications based on specific event patterns.
- Agent Configuration: Installing and configuring agents on EC2 instances, for example, AWS Systems Manager Agent (SSM Agent) and CloudWatch agent.
- AWS Config Rules: Configuring AWS Config rules to address issues.
- Health Checks: Configuring health checks using services like Route 53 and ALB.

Incident and Event Response

- AWS Event Integration: Integrating AWS event sources, including AWS Health, EventBridge, and CloudTrail.
- Event Processing: Creating event processing workflows with services like Amazon SQS, Kinesis, SNS, Lambda, and Step Functions.
- Configuration Changes: Applying configuration changes to systems in response to events.
- Infrastructure Modifications: Modifying infrastructure configurations based on events.
- Remediation: Fixing undesired system states.
- Deployment Analysis: Analyzing failed deployments, such as AWS CodePipeline, CodeBuild, CodeDeploy, CloudFormation, and CloudWatch synthetic monitoring.
- Incident Analysis: Analyzing incidents related to failed processes, such as auto scaling, Amazon ECS, and Amazon EKS.

Security and Compliance

- Least Privilege Policies: Designing policies to enforce least privilege access.
- Access Control Patterns: Implementing role-based and attribute-based access control patterns.
- Credential Rotation: Automating credential rotation for machine identities using Secrets Manager.
- Permissions Management: Managing permissions to control access for both human and machine identities, with features like MFA, AWS STS, and IAM profiles.
- Security Controls Automation: Automating

security controls application in multi-account and multi-Region environments, involving services like Security Hub, Organizations, AWS Control Tower, and Systems Manager.

- Defense in Depth: Combining security controls to create defense in depth, with services such as ACM, AWS WAF, AWS Config, GuardDuty, security groups, network ACLs, Amazon Detective, and Network Firewall.
- Sensitive Data Discovery: Automatically discovering sensitive data at scale, for example, with Amazon Macie.
- Data Encryption: Encrypting data in transit and at rest using AWS KMS, AWS CloudHSM, and ACM.
- Security Auditing: Implementing thorough security auditing.
- Alert Configuration: Configuring alerts for unexpected or anomalous security events.
- Logging and Analysis: Configuring service and application logging, including CloudTrail and CloudWatch Logs, and analyzing logs, metrics, and security findings.

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC