INFOSEC Skills
LIVE BOOT CAMPS

# Get live, expert instruction from anywhere.

# Cloud Operations on AWS Boot Camp

The Cloud Operations on AWS course is designed for systems operators on how to manage and operate automatable and repeatable deployments of networks and systems on AWS with hands-on exercises to help you learn by doing.

## Course description

This 3-day Boot Camp is focused on teaching you fundamental applications in the areas of applying networking concepts, implementing architectural requirements, monitoring, logging and troubleshooting systems and more.

This boot camp not only teaches you the knowledge and skills of AWS systems and operations management, it also prepares you to successfully pass the challenging AWS Certified SysOps Administrator – Associate 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

» System administrators and operators who are operating in the AWS Cloud

» Informational technology workers who want to increase their cloud operations knowledge

## Boot camp at a glance

### What you'll learn

- ✓ Support and maintain AWS workloads according to the AWS Well-Architected Framework.
- ✓ Perform operations by using the AWS Management Console and the AWS CLI.
- ✓ Implement security controls to meet compliance requirements.

### 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 Cloud Operations on AWS Boot Camp, it is recommended that you have completed the AWS Technical Essentials course, with a background in software development or systems administration, proficiency in maintaining operating systems at the command line (including shell scripting in Linux environments or cmd/PowerShell in Windows), and basic knowledge of networking protocols (TCP/IP, HTTP).

## Exam objectives

This boot camp prepares you to pass AWS Certified SysOps Administrator – Associate (SOA-C02) exam, which covers 6 domain areas designed to ensure relevancy across all disciplines of information security.

- Domain 1: Monitoring, Logging, and Remediation
- Domain 2: Reliability and Business Continuity
- Domain 3: Deployment, Provisioning, and Automation
- Domain 4: Security and Compliance
- Domain 5: Networking and Content Delivery
- Domain 6: Cost and Performance Optimization

## 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.

# Cloud Operations 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<br>Intro to (SOA-C02)<br>Domain 1: Monitoring, Logging, and Remediation | Domain 3: Deployment, Provisioning, and Automation | Domain 5: Networking and Content Delivery |
| Afternoon session | Domain 2: Reliability and Business Continuity | Domain 4: Security and Compliance | Domain 6: Cost and Performance Optimization<br>Recap & Review<br>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

### Monitoring, Logging, and Remediation

- Logs Management: Identify, gather, assess, and export logs, including Amazon CloudWatch Logs, CloudWatch Logs Insights, and AWS CloudTrail logs.
- Metrics and Logs Collection: Collect metrics and logs using the CloudWatch agent to monitor system performance.
- Alerting with Alarms: Establish CloudWatch alarms to be alerted when certain conditions are met.
- Metric Filters: Create filters for specific metrics to narrow down the focus of your monitoring.
- Custom Dashboards: Build customized CloudWatch dashboards to visualize and analyze data.
- Notification Configuration: Set up various notification channels such as Amazon SNS, Service Quotas, CloudWatch alarms, and AWS Health events.
- Troubleshooting and Remediation: Address issues and take corrective actions based on received notifications and alarms.
- Event-Driven Actions: Configure Amazon EventBridge rules to trigger specific actions in response to events.
- Automation for Compliance: Utilize AWS Systems Manager Automation runbooks to automate responses based on AWS Config rules, ensuring compliance and system integrity.

### Reliability and Business Continuity

- Auto Scaling Plans: Develop and maintain AWS Auto Scaling plans for dynamic resource management.
- Caching Implementation: Incorporate caching techniques to enhance system performance.
- Database Replicas: Utilize Amazon RDS replicas and Amazon Aurora Replicas to enhance data resilience.
- Loosely Coupled Architectures: Implement loosely coupled architectures to improve system stability.
- Scaling Differentiation: Distinguish between horizontal scaling and vertical scaling strategies.

- Load Balancing and Health Checks: Configure Elastic Load Balancing (ELB) and Amazon Route 53 health checks for efficient traffic distribution.
- Availability Zones: Understand and differentiate between single Availability Zone and Multi-AZ deployments across various AWS services.
- Fault-Tolerant Workloads: Implement fault-tolerant workloads, including Amazon Elastic File System (EFS) and Elastic IP addresses.
- Route 53 Routing Policies: Implement Route 53 routing policies like failover, weighted routing, and latency-based routing.
- Snapshot Automation: Automate snapshots and backups, considering use cases such as RDS snapshots, AWS Backup, RTO and RPO, Amazon Data Lifecycle Manager, and retention policies.
- Database Restoration: Learn how to restore databases, including point-in-time restoration and promoting read replicas.
- Data Management: Implement versioning and lifecycle rules for effective data management, along with configuring Amazon S3 Cross-Region Replication (CRR).
- Disaster Recovery: Understand and perform disaster recovery procedures to ensure business continuity.

## Deployment, Provisioning, and Automation

- AMI Management: Create and manage Amazon Machine Images (AMIs), possibly using EC2 Image Builder.
- CloudFormation Expertise: Gain proficiency in creating, managing, and troubleshooting AWS CloudFormation templates.
- Resource Provisioning: Provision resources across multiple AWS Regions and accounts through tools like AWS Resource Access Manager (AWS RAM), CloudFormation StackSets, and IAM cross-account roles.
- Deployment Strategies: Select deployment scenarios and services, including blue/green, rolling, and canary deployments.
- Deployment Issue Remediation: Identify and address deployment issues, which might include service quotas, subnet sizing, CloudFormation errors, and permissions.
- Automation Tools: Leverage AWS services like Systems Manager and CloudFormation for automating deployment processes.
- Patch Management: Implement automated patch management to keep systems up to date.
- Task Scheduling: Schedule automated tasks using AWS services such as EventBridge and AWS Config for streamlined operations.

## Security and Compliance

- IAM Implementation: Deploy IAM features like password policies, multi-factor authentication (MFA), roles, SAML, federated identity, resource policies, and policy conditions.
- Access Issue Handling: Resolve and audit access problems using AWS tools such as CloudTrail, IAM Access Analyzer, and IAM policy simulator.
- Policy Validation: Verify service control policies (SCPs) and permissions boundaries.
- Security Checks Review: Examine AWS Trusted Advisor security checks.
- Compliance-Based Choices: Ensure AWS Region and service selections align with compliance requirements.
- Multi-Account Security: Implement secure multi-account strategies, for example, using AWS Control Tower and AWS Organizations.
- Data Classification: Enforce a data classification system.
- Encryption Management: Create, manage, and safeguard encryption keys.
- Encryption Implementation: Apply encryption at rest with AWS Key Management Service (AWS KMS) and in transit using AWS Certificate Manager (ACM) and VPN.
- Secrets Security: Securely store secrets using AWS services such as AWS Secrets Manager and Systems Manager Parameter Store.

» Security Reports: Review reports and findings from AWS Security Hub, Amazon GuardDuty, AWS Config, and Amazon Inspector.

### Networking and Content Delivery

» VPC Configuration: Set up a Virtual Private Cloud (VPC) with components like subnets, route tables, network ACLs, security groups, NAT gateway, and internet gateway.
» Private Connectivity: Configure private connectivity options like Systems Manager Session Manager, VPC endpoints, VPC peering, and VPN.
» Network Protection: Enable AWS network protection services such as AWS WAF and AWS Shield.
» DNS Configuration: Set up Route 53 hosted zones, records, routing policies (e.g., geolocation, geoproximity), and Route 53 Resolver for DNS management.
» Content Delivery: Configure Amazon CloudFront and S3 origin access control (OAC), as well as S3 static website hosting.
» VPC Analysis: Interpret VPC configurations, including subnets, route tables, network ACLs, and security groups.
» Log Collection: Gather and interpret logs from sources like VPC Flow Logs, ELB access logs, AWS WAF web ACL logs, and CloudFront logs.
» Caching Troubleshooting: Identify and resolve caching issues in CloudFront.
» Connectivity Issues: Troubleshoot problems related to hybrid and private connectivity.

### Cost and Performance Optimization

» Cost Tagging: Utilize cost allocation tags for effective cost tracking.
» Resource Efficiency: Identify and rectify the underutilization or non-use of resources through AWS tools like Trusted Advisor, AWS Compute Optimizer, and AWS Cost Explorer.
» Budget Management: Set up AWS Budgets and billing alarms to control and monitor expenses.
» Spot Instances: Assess usage patterns to determine which workloads can benefit from EC2 Spot Instances.
» Managed Services: Explore the use of managed services such as Amazon RDS, AWS Fargate, and Amazon EFS to enhance efficiency.
» Performance-Driven Recommendations: Suggest appropriate compute resources based on performance metrics.
» EBS Optimization: Monitor and adjust Amazon Elastic Block Store (EBS) configurations to improve performance efficiency.
» S3 Performance Enhancements: Implement performance features like S3 Transfer Acceleration and multipart uploads for Amazon S3.
» RDS Performance Monitoring: Monitor RDS metrics and make configuration changes to enhance performance efficiency, including tools like Performance Insights and RDS Proxy.
» EC2 Enhancement: Activate enhanced EC2 capabilities, including Elastic Network Adapter, instance store, and placement groups for better performance.

## 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