

JON BONSO AND IRENE BONSO

**AWS CERTIFIED
DEVOPS
ENGINEER
PROFESSIONAL**



Tutorials Dojo Study Guide



TABLE OF CONTENTS

INTRODUCTION	8
AWS CERTIFIED DEVOPS ENGINEER PROFESSIONAL EXAM OVERVIEW	9
Exam Details	10
Exam Domains	11
Exam Domain I: SDLC Automation	12
Exam Domain II: Configuration Management and IaC	14
Exam Domain III: Resilient Cloud Solutions	15
Exam Domain IV: Monitoring and Logging	17
Exam Domain V: Incident and Event Response	19
Exam Domain VI: Security and Compliance	20
Old DOP-C01 vs the New DOP-C02 Exam Version	22
Exam Scoring System	23
Related Exam Topics	24
Excluded Exam Topics	27
Exam Benefits	27
AWS CERTIFIED DEVOPS ENGINEER PROFESSIONAL EXAM - STUDY GUIDE AND TIPS	28
Study Materials	28
AWS Services to Focus On	30
Common Exam Scenarios	31
Validate Your Knowledge	37
Sample Question 1	38
Sample Question 2	40
Domain 1: Software Development Life Cycle (SDLC) Automation	44
Overview	45
What is DevOps?	46
A Brief History of the DevOps Exam in AWS	48
Why Automate?	49
Types of Blue Green Deployment via ELB, Route 53, Elastic Beanstalk	50
AWS Lambda Function Alias Traffic Shifting	55
Basic Blue/Green Deployment using Route 53	58
Lifecycle Event Hook Availability (CodeDeploy Concept)	60
Automatically Run CodeBuild Tests After a Developer Creates a Pull Request	63
Automating Pull Request Validation with AWS CodeBuild	63



DevOps Exam Notes:	63
Automated Pull Request Validation Workflow	63
Managing Artifacts in AWS CodeBuild and CodePipeline	65
DynamoDB – Fetch vs Projected Attributes	71
CodeBuild with CloudWatch Logs, Metrics, and Alarms	73
CodeDeploy with CloudWatch Logs, Metrics, and Alarms	82
CodePipeline and Amazon EventBridge Integration	91
CodeDeploy - Linear, Canary and All-at-Once (Pre-defined Deployments)	94
Elastic Beanstalk - Deployment Policies and Settings	96
Domain 2: Configuration Management and Infrastructure-as-Code	99
Overview	100
What is Configuration Management?	101
What is Infrastructure-as-Code (IaC)?	102
CloudFormation Cross-Stack Reference	103
Lambda Function Artifact from S3 or CloudFormation Inline	105
AutoScalingReplacingUpdate vs AutoScalingRollingUpdate Policy	108
Discovery Agent vs Discovery Connector	110
CloudFormation Template for ECS, Auto Scaling and ALB	111
Domain 3: Resilient Cloud Solutions	113
Overview	114
High Availability vs. Fault Tolerance	115
Multi-AZ vs Multi-Region Architecture	117
Disaster Recovery Objectives	118
Amazon Route 53 Routing Policies	120
Amazon RDS Disaster Recovery Strategies	122
Auto Scaling Group with MinSize = 1 and MaxSize = 1	125
Auto Scaling Lifecycle Hooks	128
Amazon EKS Auto Scaling	130
Amazon EKS Networking	136
Automated Patching for Hybrid Environments	143
Amazon EC2 Image Builder	149
Automated RDS Read Replica Promotion	157
Amazon S3 Object tagging and Access control	161
Amazon Storage Gateway - S3 File Gateway	166
Amazon CodeGuru Reviewer	169
Amazon CodeGuru Profiler	174



Domain 4: Monitoring and Logging	179
Overview	180
AWS Config Multi-Account Multi-Region Data Aggregation	181
Consolidating VPC Flow Logs From Multiple Sources	182
Consolidating CloudTrail Log Files from Multiple Sources	184
Ensuring the Integrity of the CloudTrail Log Files	186
Fetching Application Logs from Amazon EC2, ECS and On-premises Servers	187
CloudWatch Logs Agent to CloudWatch Logs Subscription	189
Monitoring Service Limits with Trusted Advisor	191
Domain 5: Incident and Event Response	195
Overview	196
Incident and Event Response Management on AWS	197
Amazon S3 Event Notifications	199
Amazon RDS Event Notifications	201
AWS_RISK_CREDENTIALS_EXPOSED Event	202
AWS-Scheduled Maintenance Notification to Slack Channel	206
Using AWS Health API and Amazon EventBridge for Monitoring AWS-Scheduled Deployments/Changes	209
Monitoring Amazon EC2 Auto Scaling Events	211
Monitoring Amazon S3 Data Events in AWS CloudTrail	213
AWS CodePipeline Event Patterns	214
Monitoring Deployments in AWS CodeDeploy	217
Orchestrating Events in AWS CodePipeline	218
Domain 6: Security and Compliance	220
Overview	221
Management and Governance on AWS	222
AWS CodeBuild Configuration Best Practices	226
S3 Bucket Policy to Only Allow HTTPS Requests	228
Secrets Manager vs. Systems Manager Parameter Store	230
AWS Managed Policy	231
Using Systems Manager Automation to create AMIs	234
AWS SSM Session Manager to Record Sessions on your Instances	236
AWS Systems Manager Inventory	240
Systems Manager Patch Manager and Maintenance Windows	244
AWS IAM Identity Center	249
RELATED AWS SERVICES TO FOCUS	250
Amazon Elastic MapReduce (EMR)	251



Amazon Quick (formerly Amazon QuickSight)	251
Amazon Kinesis Data Streams	251
Amazon AppFlow	252
Amazon Eventbridge	252
AWS App Runner	252
AWS App2Container	253
Amazon EKS Deployment Options	253
Amazon EKS on AWS Outposts	253
Amazon EKS Distro	254
Red Hat OpenShift Service on AWS (ROSA)	254
AWS Database Migration Service (AWS DMS)	254
Amazon DocumentDB (with MongoDB compatibility)	254
Amazon MemoryDB for Redis	255
Amazon ElastiCache	255
AWS Command Line Interface (AWS CLI)	256
AWS Cloud Development Kit (AWS CDK)	256
AWS CloudShell	256
AWS CodeArtifact	257
Amazon CodeGuru	257
AWS Fault Injection Simulator (AWS FIS)	258
AWS Control Tower	258
Customizations for AWS Control Tower (CfCT)	258
Amazon Compute Optimizer	259
Amazon Managed Grafana	259
Amazon Managed Service for Prometheus	260
Amazon FSx	260
AWS Backup	261
AWS Elastic Disaster Recovery	261
AWS Proton	262
AWS CloudHSM	262
AWS Network Firewall	262
Amazon Detective	263
Amazon Cognito	263
AWS Virtual Private Network (AWS VPN)	264
AWS PrivateLink	264
AWS License Manager	265



AWS Service Health Dashboard	265
AWS Health API	265
AWS Resilient Hub	265
AWS CHEAT SHEETS	266
AWS Compute Services	267
Amazon Elastic Compute Cloud (EC2)	267
Amazon Elastic Container Registry (ECR)	270
Amazon Elastic Container Service (ECS)	271
AWS Elastic Beanstalk	273
AWS Lambda	274
AWS Serverless Application Model (SAM)	275
AWS Serverless Application Repository	276
AWS Storage Services	277
Amazon EBS	277
Amazon EFS	277
Amazon S3	277
Amazon S3 Bucket Policies for VPC Endpoints	279
Amazon S3 Glacier Flexible Retrieval (formerly S3 Glacier)	280
AWS Storage Gateway	281
AWS Database Services	283
Amazon Aurora	283
Aurora Serverless v2	284
Amazon DynamoDB	285
Lambda Integration With Amazon DynamoDB Streams	286
Amazon RDS	288
Amazon Redshift	290
AWS Networking & Content Delivery	291
Amazon API Gateway	291
Amazon Route 53	292
Amazon CloudFront	294
AWS Elastic Load Balancing (ELB)	295
AWS Transit Gateway	296
AWS Security & Identity Services	297
Amazon GuardDuty	297
Amazon Inspector	298
Amazon Macie	299



AWS Identity & Access Management (IAM)	300
AWS Key Management Service	303
AWS Secrets Manager	304
AWS Certificate Manager	305
AWS Directory Service	308
AWS Resource Access Manager	313
AWS Security Hub	314
AWS Security Token Service (AWS STS)	315
AWS Shield	316
AWS WAF	318
AWS Management Tools	319
AWS Organizations	319
Amazon CloudWatch	321
AWS Auto Scaling	323
AWS CloudFormation	325
AWS CloudTrail	328
AWS Config	329
AWS Health	331
AWS Systems Manager	331
AWS Trusted Advisor	335
AWS Service Catalog	335
AWS Analytics Services	338
Amazon OpenSearch Service	338
Amazon Kinesis	340
Amazon Athena	343
AWS Developer Tools	345
AWS CodeBuild	345
AWS CodeDeploy	347
AWS CodePipeline	351
AWS X-Ray	353
AWS SDKs and Tools	353
AWS Application Services	354
Amazon SNS	354
AWS Step Functions	356
Comparison of AWS Services	358
AWS CloudTrail vs Amazon CloudWatch	358



CloudWatch Agent vs SSM Agent vs Custom Daemon Scripts	359
EC2 Container Services ECS vs Lambda	360
EC2 Instance Health Check vs ELB Health Check vs Auto Scaling and Custom Health Check	362
Elastic Beanstalk vs CloudFormation vs CodeDeploy	365
Service Control Policies vs IAM Policies	367
FINAL REMARKS AND TIPS	369
ABOUT THE AUTHORS	370



INTRODUCTION

As more companies build their DevOps practices, there will always be a growing demand for certified IT Professionals that can do agile software development, configuration management, task automation, and continuous integration/continuous delivery (CI/CD). This Study Guide and Cheat Sheets eBook for AWS Certified DevOps Engineer - Professional aims to equip you with the necessary knowledge and practical skill sets needed to pass the latest version of the AWS Certified DevOps Engineer – Professional exam.

This eBook contains the essential concepts, exam domains, exam tips, sample questions, cheat sheets, and other relevant information about the AWS Certified DevOps Engineer – Professional exam. This study guide begins with the presentation of the exam structure, giving you an insight into the question types, exam domains, scoring scheme, and the list of benefits you'll receive once you pass the exam. We used the official AWS [exam guide](#) to structure the contents of this guide, where each section discusses a particular exam domain. Various DevOps concepts, related AWS services, and technical implementations are covered to provide you with an idea of what to expect on the actual exam.

DevOps Exam Notes:

Don't forget to read the boxed "**exam tips**" (like this one) scattered throughout the eBook, as these are the key concepts that you will likely encounter on your test. After covering the six domains, we have added a bonus section containing a curated list of AWS Cheat Sheets to fast-track your review. The last part of this guide includes a collection of articles that compares two or more similar AWS services to supplement your knowledge.

The AWS Certified DevOps Engineer - Professional certification exam is a difficult test to pass; therefore, anyone who wants to take it must allocate ample time for review. The exam registration cost is not cheap, which is why we spent considerable time and effort to ensure that this study guide provides you with the essential and relevant knowledge to increase your chances of passing the DevOps exam.

**** Note:** *This eBook is meant to be just a supplementary resource when preparing for the exam. We highly recommend working on [hands-on sessions](#) and [practice exams](#) to further expand your knowledge and improve your test-taking skills.*



AWS CERTIFIED DEVOPS ENGINEER PROFESSIONAL EXAM OVERVIEW

The AWS Certified DevOps Engineer - Professional certification exam validates various skills which are necessary to become a full-fledged DevOps engineer. The exam will check your capability in implementing and managing continuous delivery systems and methodologies on AWS. Automating security controls, validating compliance, and optimizing the governance processes are also included in the test.

This professional-level AWS certification exam validates your technical expertise in provisioning, operating, and managing distributed systems and services on the AWS Cloud. It also verifies your ability to complete the following DevOps tasks:

- 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 AWS.
- Design, manage, and maintain tools to automate operational processes

Before we discuss the details of the new exam, it's important to know the history of this certification test to better understand the changes it entails. We will go back in time and re-discover the history of the AWS Certified DevOps Engineer Professional exam and other exam-related information.

Amazon Web Services (AWS) started its Global Certification Program in 2013, which was about a decade ago. The primary purpose of this program is to validate the necessary technical skills and knowledge required for building secure and reliable cloud-based applications using the AWS Cloud. By passing the AWS Certification exam, IT professionals can prove their expertise and knowledge in the AWS Cloud to their current employers or even to the prospective companies they wish to apply for. AWS unveiled the Professional and Specialty-level certifications in an effort to expand its certification program and continuously release new updates.

These Professional-level exams have covered various domains, namely monitoring, security, SDLC, Infrastructure as Code(IaC), data analytics, advanced networking, machine learning, and many others. There are a bunch of new and updated versions of AWS certification exams that are released on a regular basis to include the new services offered by AWS and as well as to incorporate the new knowledge areas.

There are basically two Professional-level exams offered by AWS, which are the AWS Certified Solutions Architect – Professional and the AWS Certified DevOps Engineer – Professional. The first version of the AWS Certified Solutions Architect Professional exam (SAP-C00) was released in May 2014. This was followed by the first version of the AWS Certified DevOps Engineer Professional exam (DOP-C00) on February 2015. After 4 years, an updated version of the AWS Certified DevOps Engineer – Professional certification was launched on February 2019 with an exam code of DOP-C01.



After 4 years, the AWS Certification and Training team released yet another version of this certification test with an exam code of DOP-C02. The latest version of the AWS Certified DevOps Engineer – Professional certification exam was released on the 7th day of March 2023. Based on this trend, it can be assumed that the new version of the DevOps Professional exam will be coming in around 2025 or 2026 with an exam code of DOP-C03.

Exam Details

The AWS Certified DevOps Engineer Professional certification is intended for IT Professionals who perform a Solutions Architect or DevOps role and have substantial years of hands-on experience designing available, cost-efficient, fault-tolerant, and scalable distributed systems on the AWS platform. It is composed of scenario-based questions that can either be in multiple-choice or multiple-response formats. The first question type has one correct answer and three incorrect responses, while the latter has two or more correct responses out of five or more options. You can take the exam from a local testing center or online from the comfort of your home.

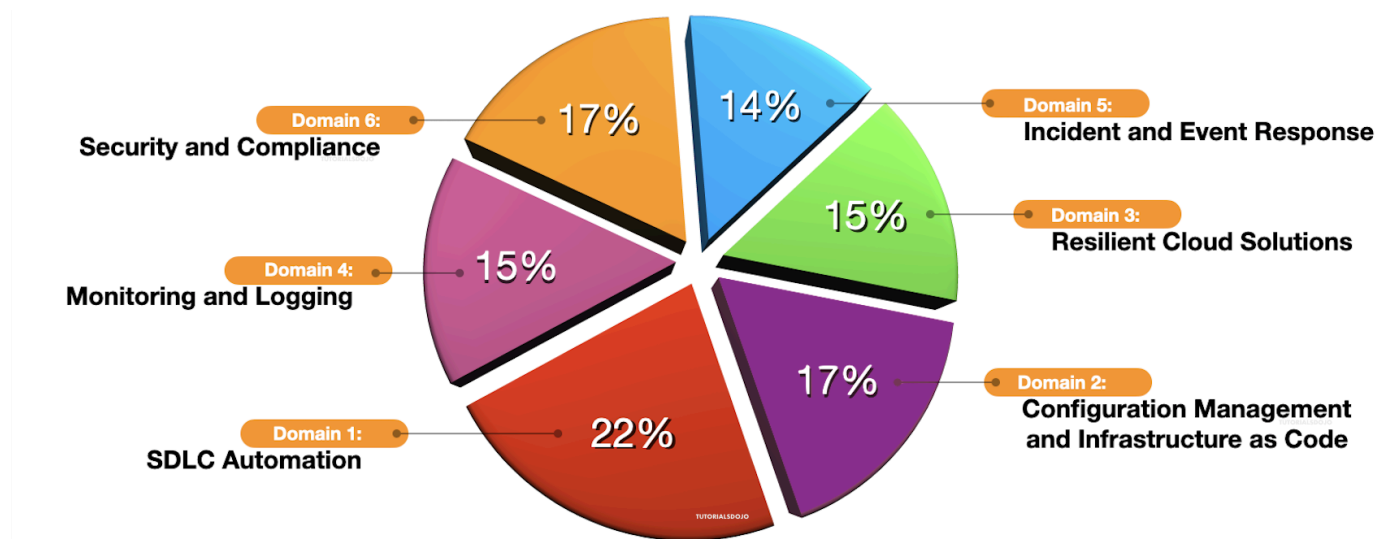
Exam Code:	DOP-C02
Release Date:	March 2023
Prerequisites:	None
No. of Questions:	75
Score Range:	100 - 1000
Passing Score:	750/1000
Time Limit:	3 hours (180 minutes)
Format:	Scenario-based. Multiple choice/multiple answers.
Delivery Method:	Testing center or online proctored exam.

Don't be confused if you see in your Pearson Vue booking that the duration is 190 minutes since they included an additional 10 minutes for reading the Non-Disclosure Agreement (NDA) at the start of the exam and the survey at the end of it.

Exam Domains

The AWS Certified DevOps Engineer Professional (DOP-C02) exam has 6 different domains, each with corresponding weight and topic coverage. The exam domains are as follows:

- Domain 1: SDLC Automation (22%)
- Domain 2: Configuration Management and IaC (17%)
- Domain 3: Resilient Cloud Solutions (15%)
- Domain 4: Monitoring and Logging (15%)
- Domain 5: Incident and Event Response (14%)
- Domain 6: Security and Compliance (17%)



The list of exam domains can be found on the official Exam Guide for the AWS Certified DevOps Engineer - Professional exam. Each exam domain is comprised of several task statements. A task statement is a sub-category of the exam domain that contains the required cloud concepts, knowledge, and skills for you to accomplish a particular task or activity in AWS.

Let's look at each of these domains one by one.



Exam Domain I: SDLC Automation

Task Statement 1: Implement CI/CD pipelines.

Knowledge of:

- Software development lifecycle (SDLC) concepts, phases, and models
- Pipeline deployment patterns for single- and multi-account environments

Skills in:

- Configuring code, image, and artifact repositories
- Using version control to integrate pipelines with application environments
- Setting up build processes (for example, AWS CodeBuild)
- Managing build and deployment secrets (for example, AWS Secrets Manager, AWS Systems Manager Parameter Store)
- Determining appropriate deployment strategies (for example, AWS CodeDeploy)

Task Statement 2: Integrate automated testing into CI/CD pipelines.

Knowledge of:

- Different types of tests (for example, unit tests, integration tests, acceptance tests, user interface tests, security scans)
- Reasonable use of different types of tests at different stages of the CI/CD pipeline

Skills in:

- Running builds or tests when generating pull requests or code merges (for example, Git, CodeBuild)
- Running load/stress tests, performance benchmarking, and application testing at scale
- Measuring application health based on application exit codes
- Automating unit tests and code coverage
- Invoking AWS services in a pipeline for testing



Task Statement 3: Build and manage artifacts.

Knowledge of:

- Artifact use cases and secure management
- Methods to create and generate artifacts
- Artifact lifecycle considerations

Skills in:

- Creating and configuring artifact repositories (for example, AWS CodeArtifact, Amazon S3, Amazon Elastic Container Registry [Amazon ECR])
- Configuring build tools for generating artifacts (for example, CodeBuild, AWS Lambda)
- Automating Amazon EC2 instance and container image build processes (for example, EC2 Image Builder)

Task Statement 4: Implement deployment strategies for instance, container, and serverless environments.

Knowledge of:

- Deployment methodologies for various platforms (for example, Amazon EC2, Amazon Elastic Container Service [Amazon ECS], Amazon Elastic Kubernetes Service [Amazon EKS], Lambda)
- Application storage patterns (for example, Amazon Elastic File System [Amazon EFS], Amazon S3, Amazon Elastic Block Store [Amazon EBS])
- Mutable deployment patterns in contrast to immutable deployment patterns
- Tools and services available for distributing code (for example, CodeDeploy, EC2 Image Builder)

Skills in:

- Configuring security permissions to allow access to artifact repositories (for example, AWS Identity and Access Management [IAM], CodeArtifact)
- Configuring deployment agents (for example, CodeDeploy agent)
- Troubleshooting deployment issues
- Using different deployment methods (for example, blue/green, canary)



Exam Domain II: Configuration Management and IaC

Task Statement 1: Define cloud infrastructure and reusable components to provision and manage systems throughout their lifecycle.

Knowledge of:

- Infrastructure as code (IaC) options and tools for AWS
- Change management processes for IaC-based platforms
- Configurations management services and strategies

Skills in:

- Composing and deploying IaC templates (for example, AWS Serverless Application Model [AWS SAM], AWS CloudFormation, AWS Cloud Development Kit [AWS CDK])
- Applying AWS CloudFormation StackSets across multiple accounts and AWS Regions
- Determining optimal configuration management services (for example, AWS Systems Manager, AWS Config, AWS AppConfig)
- Implementing infrastructure patterns, governance controls, and security standards into reusable IaC templates (for example, AWS Service Catalog, CloudFormation modules, AWS CDK)

Task Statement 2: Deploy automation to create, onboard, and secure AWS accounts in a multi-account/multi-Region environment.

Knowledge of:

- AWS account structures, best practices, and related AWS services

Skills in:

- Standardizing and automating account provisioning and configuration
- Creating, consolidating, and centrally managing accounts (for example, AWS Organizations, AWS Control Tower)
- Applying IAM solutions for multi-account and complex organization structures (for example, SCPs, assuming roles)
- Implementing and developing governance and security controls at scale (AWS Config, AWS Control Tower, AWS Security Hub, Amazon Detective, Amazon GuardDuty, AWS Service Catalog, SCPs)



Task Statement 3: Design and build automated solutions for complex tasks and large-scale environments.

Knowledge of:

- AWS services and solutions to automate tasks and processes
- Methods and strategies to interact with the AWS software-defined infrastructure

Skills in:

- Automating system inventory, configuration, and patch management (for example, Systems Manager, AWS Config)
- Developing Lambda function automation for complex scenarios (for example, AWS SDKs, Lambda, AWS Step Functions)
- Automating the configuration of software applications to the desired state (for example, Systems Manager State Manager)
- Maintaining software compliance (for example, Systems Manager)

Exam Domain III: Resilient Cloud Solutions

Task Statement 1: Implement highly available solutions to meet resilience and business requirements.

Knowledge of:

- Multi-AZ and multi-Region deployments (for example, compute layer, data layer)
- Service Level Agreements (SLAs)
- Replication and failover methods for stateful services
- Techniques to achieve high availability (for example, Multi-AZ, multi-Region)

Skills in:

- Translating business requirements into technical resiliency needs
- Identifying and remediating single points of failure in existing workloads
- Enabling cross-Region solutions where available (for example, Amazon DynamoDB, Amazon RDS, Amazon Route 53, Amazon S3, Amazon CloudFront)
- Configuring load balancing to support cross-AZ services
- Configuring applications and related services to support multiple Availability Zones and Regions while minimizing downtime



Task Statement 2: Implement solutions that are scalable to meet business requirements.

Knowledge of:

- Appropriate metrics for scaling services
- Loosely coupled and distributed architectures
- Serverless architectures
- Container platforms

Skills in:

- Identifying and remediating scaling issues
- Identifying and implementing appropriate auto-scaling, load balancing, and caching solutions
- Deploying container-based applications (for example, Amazon ECS, Amazon EKS)
- Deploying workloads in multiple AWS Regions for global scalability
- Configuring serverless applications (for example, Amazon API Gateway, Lambda, AWS Fargate)

Task Statement 3: Implement automated recovery processes to meet RTO/RPO requirements.

Knowledge of:

- Disaster recovery concepts (for example, RTO, RPO)
- Backup and recovery strategies (for example, pilot light, warm standby)
- Recovery procedures

Skills in:

- Testing failover of Multi-AZ/multi-Region workloads (for example, Amazon RDS, Amazon Aurora, Route 53, CloudFront)
- Identifying and implementing appropriate cross-Region backup and recovery strategies (for example, AWS Backup, Amazon S3, Systems Manager)
- Configuring a load balancer to recover from backend failure



Exam Domain IV: Monitoring and Logging

Task Statement 1: Configure the collection, aggregation, and storage of logs and metrics.

Knowledge of:

- How to monitor applications and infrastructure
- Amazon CloudWatch metrics (for example, namespaces, metrics, dimensions, and resolution)
- Real-time log ingestion
- Encryption options for at-rest and in-transit logs and metrics (for example, client-side and server-side, AWS Key Management Service [AWS KMS])
- Security configurations (for example, IAM roles and permissions to allow for log collection)

Skills in:

- Securely storing and managing logs
- Creating CloudWatch metrics from log events by using metric filters
- Creating CloudWatch metric streams (for example, Amazon S3 or Amazon Data Firehose options)
- Collecting custom metrics (for example, using the CloudWatch agent)
- Managing log storage lifecycles (for example, S3 lifecycles, CloudWatch log group retention)
- Processing log data by using CloudWatch log subscriptions (for example, Kinesis, Lambda, Amazon OpenSearch Service)
- Searching log data by using filter and pattern syntax or CloudWatch Logs Insights
- Configuring encryption of log data (for example, AWS KMS)

Task Statement 2: Audit, monitor, and analyze logs and metrics to detect issues.

Knowledge of:

- Anomaly detection alarms (for example, CloudWatch anomaly detection)
- Common CloudWatch metrics and logs (for example, CPU utilization with Amazon EC2, queue length with Amazon RDS, 5xx errors with an Application Load Balancer)
- Amazon Inspector and common assessment templates
- AWS Config rules
- AWS CloudTrail log events



Skills in:

- Building CloudWatch dashboards and Amazon Quick (Amazon QuickSight) visualizations.
- Associating CloudWatch alarms with CloudWatch metrics (standard and custom)
- Configuring AWS X-Ray for different services (for example, containers, API Gateway, Lambda)
- Analyzing real-time log streams (for example, using Kinesis Data Streams)
- Analyzing logs with AWS services (for example, Amazon Athena, CloudWatch Logs Insights)

Task Statement 3: Automate monitoring and event management of complex environments.

Knowledge of:

- Event-driven, asynchronous design patterns (for example, S3 Event Notifications or Amazon EventBridge events to Amazon Simple Notification Service [Amazon SNS] or Lambda)
- Capabilities of auto scaling a variety of AWS services (for example, EC2 Auto Scaling groups, RDS storage auto scaling, DynamoDB, ECS capacity provider, EKS autoscalers)
- Alert notification and action capabilities (for example, CloudWatch alarms to Amazon SNS, Lambda, EC2 automatic recovery)
- Health check capabilities in AWS services (for example, Application Load Balancer target groups, Route 53)

Skills in:

- Configuring solutions for auto scaling (for example, DynamoDB, EC2 Auto Scaling groups, RDS storage auto scaling, ECS capacity provider)
- Creating CloudWatch custom metrics and metric filters, alarms, and notifications (for example, Amazon SNS, Lambda)
- Configuring S3 events to process log files (for example, by using Lambda), and deliver log files to another destination (for example, OpenSearch Service, CloudWatch Logs)
- Configuring EventBridge to send notifications based on a particular event pattern
- Installing and configuring agents on EC2 instances (for example, AWS Systems Manager Agent [SSM Agent], CloudWatch agent)
- Configuring AWS Config rules to remediate issues
- Configuring health checks (for example, Route 53, Application Load Balancer)



Exam Domain V: Incident and Event Response

Task Statement 1: Manage event sources to process, notify, and take action in response to events.

Knowledge of:

- AWS services that generate, capture, and process events (for example, AWS Health, EventBridge, CloudTrail)
- Event-driven architectures (for example, fan out, event streaming, queuing)

Skills in:

- Integrating AWS event sources (for example, AWS Health, EventBridge, CloudTrail)
- Building event processing workflows (for example, Amazon Simple Queue Service [Amazon SQS], Kinesis, Amazon SNS, Lambda, Step Functions)

Task Statement 2: Implement configuration changes in response to events.

Knowledge of:

- Fleet management services (for example, Systems Manager, AWS Auto Scaling)
- Configuration management services (for example, AWS Config)

Skills in:

- Applying configuration changes to systems
- Modifying infrastructure configurations in response to events
- Remediating a non-desired system state

Task Statement 3: Troubleshoot system and application failures.

Knowledge of:

- AWS metrics and logging services (for example, CloudWatch, X-Ray)
- AWS service health services (for example, AWS Health, CloudWatch, Systems Manager OpsCenter)
- Root cause analysis



Skills in:

- Analyzing failed deployments (for example, AWS CodePipeline, CodeBuild, CodeDeploy, CloudFormation, CloudWatch synthetic monitoring)
- Analyzing incidents regarding failed processes (for example, auto-scaling, Amazon ECS, Amazon EKS)

Exam Domain VI: Security and Compliance

Task Statement 1: Implement techniques for identity and access management at scale.

Knowledge of:

- Appropriate usage of different IAM entities for human and machine access (for example, users, groups, roles, identity providers, identity-based policies, resource-based policies, session policies)
- Identity federation techniques (for example, using IAM identity providers and AWS IAM Identity Center)
- Permission management delegation by using IAM permissions boundaries
- Organizational SCPs

Skills in:

- Designing policies to enforce least privilege access
- Implementing role-based and attribute-based access control patterns
- Automating credential rotation for machine identities (for example, Secrets Manager)
- Managing permissions to control access to human and machine identities (for example, enabling multi-factor authentication [MFA], AWS Security Token Service [AWS STS], IAM profiles)

Task Statement 2: Apply automation for security controls and data protection.

Knowledge of:

- Network security components (for example, security groups, network ACLs, routing, AWS Network Firewall, AWS WAF, AWS Shield)
- Certificates and public key infrastructure (PKI)
- Data management (for example, data classification, encryption, key management, access controls)



Skills in:

- Automating the application of security controls in multi-account and multi-Region environments (for example, Security Hub, Organizations, AWS Control Tower, Systems Manager)
- Combining security controls to apply defense in depth (for example, AWS Certificate Manager [ACM], AWS WAF, AWS Config, AWS Config rules, Security Hub, GuardDuty, security groups, network ACLs, Amazon Detective, Network Firewall)
- Automating the discovery of sensitive data at scale (for example, Amazon Macie)
- Encrypting data in transit and data at rest (for example, AWS KMS, AWS CloudHSM, ACM)

Task Statement 3: Implement security monitoring and auditing solutions.

Knowledge of:

- Security auditing services and features (for example, CloudTrail, AWS Config, VPC Flow Logs, CloudFormation drift detection)
- AWS services for identifying security vulnerabilities and events (for example, GuardDuty, Amazon Inspector, IAM Access Analyzer, AWS Config)
- Common cloud security threats (for example, insecure web traffic, exposed AWS access keys, S3 buckets with public access enabled or encryption disabled)

Skills in:

- Implementing robust security auditing
- Configuring alerting based on unexpected or anomalous security events
- Configuring service and application logging (for example, CloudTrail, CloudWatch Logs)
- Analyzing logs, metrics, and security findings

Old DOP-C01 vs the New DOP-C02 Exam Version

In terms of the number of exam domains, the old version of the AWS Certified DevOps Engineer Professional (DOP-C01) has the exact same number of domains as compared with the new DOP-C02 version. However, there are differences in terms of exam coverage and names for some domains.

The biggest exam domain is still the SDLC (Software Development Lifecycle) Automation domain which retains its 22% percent exam coverage. The same goes for the Monitoring and Logging domain, which still has 15 percent. This is followed by the Configuration Management and Infrastructure as Code (IaC) domain which is down to only 17% exam coverage from the previous 19% percent. The Incident and Event Response domain has a huge 4% decline as it only has 14% coverage coming from an 18% high on the previous version.

You can also notice that two exam domains have changed their name:

- The **"High Availability, Fault Tolerance, and Disaster Recovery"** domain has been renamed and is now called the **"Resilient Cloud Solutions"** domain.
- The **"Policies and Standards Automation"** domain is now **"Security and Compliance"**

DOP-C01 Valid until March 6, 2023		aws certified DevOps Engineer PROFESSIONAL	DOP-C02 NEW Available on March 7, 2023	
DOMAIN	% of Examination		DOMAIN	% of Examination
SDLC Automation	22%		SDLC Automation	22%
Configuration Management and Infrastructure as Code	19%		Configuration Management and Infrastructure as Code	17% ↓
Incident and Event Response	18%		RENAMED Security and Compliance	17% ↑
High Availability, Fault Tolerance, and Disaster Recover	16%		RENAMED Resilient Cloud Solutions	15% ↓
Monitoring and Logging	15%		Monitoring and Logging	15%
Policies and Standards Automation	10%		Incident and Event Response	14% ↓

- There is no BETA exam for the DOP-C02 exam version



The concept of resiliency is related to High Availability, Fault Tolerance, and Disaster Recovery. This is the primary reason why AWS renamed this lengthy domain as “Resilient Cloud Solutions” for brevity. From 16%, this exam domain has a slight decrease of coverage at 15% percent.

Security in AWS can be implemented through IAM Policies, Service Control Policies (SCPs), Bucket Policies, VPC Endpoint Policies, and other types of policies. The term “standards” is synonymous with the word “compliance” in the IT industry. The name of the Policies and Standards Automation exam domain was simplified and is now officially the Security and Compliance domain. It’s interesting to note that on the previous DOP-C01 version, this domain has the lowest exam coverage at 10%, but now, it has become the second largest exam domain for DOP-C02 with 17% coverage.

As you can notice, the DevOps Pro exam has significantly included many security-related topics based on its new exam domain content distribution. This means that you have to focus on various security topics and security services offered by AWS.

Exam Scoring System

You can get a score from 100 to 1,000 with a minimum passing score of **750** when you take the DevOps Engineer Professional exam. AWS uses a scaled scoring model to equate scores across multiple exam types that may have different difficulty levels. The complete score report will be sent to you by email after a few days. Right after you complete the actual exam, you’ll immediately see a pass or fail notification on the testing screen. A *“Congratulations! You have successfully passed...”* message will be shown if you pass the exam.

Individuals who unfortunately do not pass the AWS exam must wait 14 days before they are allowed to retake the exam. Fortunately, there is no hard limit on exam attempts until you pass the exam. Take note that on each attempt, the full registration price of the AWS exam must be paid.

Within 5 business days of completing your exam, your AWS Certification Account will have a record of your complete exam results. The score report contains a table of your performance at each section/domain, which indicates whether you met the competency level required for these domains or not. AWS is using a compensatory scoring model, which means that you do not necessarily need to pass each and every individual section, only the overall examination. Each section has a specific score weighting that translates to the number of questions; hence, some sections have more questions than others. The Score Performance table highlights your strengths and weaknesses that you need to improve on.



Related Exam Topics

The new AWS Certified DevOps Engineer – Professional exam (DOP-C02) is focused on the various tools, services, and knowledge areas that revolve around DevOps in AWS. The official exam guide provides a list of AWS services, general tools, and technologies that are grouped according to their primary functions. Keep in mind that even though some of these topics will likely be covered more than others on the exam, the placement or order of these exam topics/ AWS services in this list is not an indication of any relative weight or importance.

The relevant exam topics that you should be familiar with on your upcoming DOP-C02 exam are:

- Application Deployment
- Application Integration
- Application pipelines
- Automation
- Code repository best practices
- Cost optimization
- Deployment requirements
- Hybrid deployments
- IAM policies
- Metrics, monitoring, alarms, and logging
- Network ACL and security group design and implementation
- Operational best practices
- Rollback procedures



Here is the list of relevant AWS services that are covered in the AWS Certified DevOps Engineer – Professional (DOP-C02) exam based on the official exam guide. You must focus on these AWS services and their respective features for your upcoming test:

Analytics: • Amazon Athena • Amazon Elastic MapReduce (Amazon EMR) • Amazon Data Firehose • Amazon Kinesis Data Streams • Amazon OpenSearch Service • Amazon Quick (Amazon QuickSight) Application Integration: • Amazon AppFlow • Amazon EventBridge Compute: • AWS App Runner • Amazon EC2 • Amazon EC2 Auto Scaling • EC2 Image Builder • AWS Elastic Beanstalk • AWS Serverless Application Repository Containers: • AWS App2Container • Amazon Elastic Container Registry (Amazon ECR) • Amazon Elastic Container Service (Amazon ECS) • Amazon Elastic Kubernetes Service (Amazon EKS) • Amazon EKS Distro • AWS Fargate • Red Hat OpenShift Service on AWS (ROSA) Database: • Amazon Aurora • Amazon Aurora Serverless v2 • AWS Database Migration Service (AWS DMS) • Amazon DocumentDB (with MongoDB compatibility) • Amazon DynamoDB • Amazon ElastiCache • Amazon MemoryDB for Redis • Amazon RDS • Amazon Redshift Developer Tools:	Management and Governance: • AWS Auto Scaling • AWS CloudFormation • AWS CloudTrail • Amazon CloudWatch • Amazon CloudWatch Logs • AWS Compute Optimizer • AWS Config • AWS Control Tower • AWS Health • AWS License Manager • Amazon Managed Grafana • Amazon Managed Service for Prometheus • AWS Organizations • AWS Proton • AWS Resilience Hub • AWS Service Catalog • AWS Systems Manager • AWS Trusted Advisor Networking and Content Delivery: • Amazon API Gateway • AWS Client VPN • Amazon CloudFront • Elastic Load Balancing (ELB) • AWS PrivateLink • AWS Site-to-Site VPN • Amazon Route 53 • AWS Transit Gateway • Amazon VPC Serverless: • AWS Lambda • AWS Serverless Application Model (AWS SAM) • Amazon Simple Notification Service (Amazon SNS) • Amazon Simple Queue Service (Amazon SQS) • AWS Step Functions Security, Identity, and Compliance: • AWS Certificate Manager (ACM) • AWS CloudHSM • Amazon Cognito • Amazon Detective
---	--



- AWS Cloud Development Kit (AWS CDK)
- AWS CloudShell
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- AWS Command Line Interface (AWS CLI)
- AWS Fault Injection Simulator
- AWS SDKs and Tools
- AWS X-Ray

- AWS Directory Service
- Amazon GuardDuty
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Resource Access Manager (AWS RAM)
- AWS Secrets Manager
- AWS Security Hub
- AWS Security Token Service (AWS STS)
- AWS Shield
- AWS IAM Identity Center
- AWS WAF

Storage:

- AWS Backup
- Amazon Elastic Block Store (Amazon EBS)
- AWS Elastic Disaster Recovery (AWS DRS)
- Amazon Elastic File System (Amazon EFS)
- Amazon FSx for Lustre
- Amazon FSx for NetApp ONTAP
- Amazon FSx for OpenZFS
- Amazon FSx for Windows File Server
- Amazon S3
- Amazon S3 Glacier Flexible Retrieval (formerly S3 Glacier)
- AWS Storage Gateway



Excluded Exam Topics

Usually, the official exam guides provide a list of both the relevant and irrelevant AWS services for the exam. This is not the case for the latest AWS Certified DevOps Engineer Professional DOP-C02 exam. The official DOP-C02 exam guide doesn't come with a list of exam topics that are not in scope for this certification test. However, we can deduce the out-of-scope AWS topics by comparing the [exam guide for the AWS Certified Solutions Architect – Professional SAP-C02 exam](#).

Just a friendly reminder that the following AWS services and features do not represent each and every AWS offering that is excluded from the DOP-C02 exam content. This list is only a hint of what topics are not covered on the AWS Certified DevOps Engineer – Professional exam, which you should not focus on:

- Machine Learning
- Internet-of-Things (IoT)
- Frontend development for mobile apps
- 12-factor app methodology
- AWS Direct Connect

Exam Benefits

If you successfully passed any AWS exam, you will be eligible for the following benefits:

- **Exam Discount** - You'll get a 50% discount voucher that you can apply for your recertification or any other exam you plan to pursue. To access your discount voucher code, go to the "Benefits" section of your AWS Certification Account, and apply the voucher when you register for your next exam.
- **Certification Digital Badges** - You can showcase your achievements to your colleagues and employers with digital badges on your email signatures, LinkedIn profile, or on your social media accounts. You can also show your Digital Badge to gain exclusive access to Certification Lounges at AWS re:Invent, regional Appreciation Receptions, and select AWS Summit events. To view your badges, simply go to the "Digital Badges" section of your AWS Certification Account.



AWS CERTIFIED DEVOPS ENGINEER PROFESSIONAL EXAM - STUDY GUIDE AND TIPS

This certification is the pinnacle of your DevOps career in AWS. The AWS Certified DevOps Engineer Professional (or AWS DevOps Pro) is the advanced certification of both [AWS SysOps Administrator Associate](#) and [AWS Developer Associate](#). This is similar to how the AWS Solutions Architect Professional role is a more advanced version of the AWS Solutions Architect Associate.

Generally, AWS recommends that you first take (and pass) both AWS SysOps Administrator Associate and AWS Developer Associate certification exams before taking on this certification. Previously, it was a prerequisite that you obtain the associate level certifications before you are allowed to go for the professional level. Last October 2018, AWS removed this ruling to provide customers with a more flexible approach to the certifications.

Study Materials

The [FREE AWS Exam Readiness course](#), [official AWS sample questions](#), Whitepapers, FAQs, AWS Documentation, Re:Invent videos, forums, labs, [AWS cheat sheets](#), [practice tests](#), and personal experiences are what you will need to pass the exam. Since the DevOps Pro is one of the most difficult AWS certification exams out there, you have to prepare yourself with every study material you can get your hands on. If you need a review on the fundamentals of AWS DevOps, then do check out our review guides for the [AWS SysOps Administrator Associate](#) and [AWS Developer Associate](#) certification exams. Also, visit this [AWS exam blueprint](#) to learn more details about your certification exam.

For virtual classes, you can attend the [DevOps Engineering on AWS](#) and [Systems Operations on AWS](#) classes since they will teach you concepts and practices that are expected to be in your exam.

For whitepapers, focus on the following:

1. [Running Containerized Microservices on AWS](#)
2. [Microservices on AWS](#)
3. [Infrastructure as Code](#)
4. [Introduction to DevOps](#)
5. [Practicing Continuous Integration and Continuous Delivery on AWS](#)
6. [Jenkins on AWS](#)
7. [Blue/Green Deployments on AWS whitepaper](#)
8. [Development and Test on AWS](#)

Almost all online training you need can be found on the AWS web page. One digital course that you should check out is the [Exam Readiness: AWS Certified DevOps Engineer – Professional](#) course. This digital course

contains lectures on the different domains of your exam, and they also provide a short quiz right after each lecture to validate what you have just learned.

Exam Readiness:
AWS Certified
DevOps Engineer -
Professional

13% COMPLETE

- Course Overview ✓
- Domain 1: SDLC Automation ○
- Domain 2: Configuration Management and Infrastructure as ... ○
- Domain 3: Monitoring and Logging ○
- Domain 4: Policies and Standards Automation ○
- Domain 5: Incident and Event ○

AWS CloudFormation: update options

- MaxBatchSize:** maximum number of instances that are updated
- MinInstancesInService:** minimum number of instances that must be in service within the Auto Scaling group while old instances are updated
- PauseTime:** amount of time given to instances to start applications

```

"Resources": {
  "WebServerGroup": {
    "Type": "AWS::AutoScaling::AutoScalingGroup",
    "CreationPolicy": {
      "ResourceSignal": {
        "Timeout": "PT15M",
        "Count": "2"
      }
    }
  },
  "UpdatePolicy": {
    "AutoScalingRollingUpdate": {
      "MaxBatchSize": "1",
      "MinInstancesInService": "1",
      "PauseTime": "PT15M",
      "WaitOnResourceSignals": "true"
    }
  }
},

```

SAMPLE QUESTIONS

Lastly, do not forget to study the AWS CLI, SDKs, and APIs. Since DevOps Pro is also an advanced certification for Developer Associate, you need to have knowledge of programming and scripting in AWS. Go through the AWS documentation to review the syntax of the CloudFormation template, Serverless Application Model template, CodeBuild buildspec, CodeDeploy appspec, and IAM Policy.

Also, check out this article: [Top 5 FREE AWS Review Materials](#).



AWS Services to Focus On

Since this exam is a professional level one, you should already have a deep understanding of the AWS services listed under our SysOps Administrator Associate and Developer Associate review guides. In addition, you should familiarize yourself with the following services since they commonly come up in the DevOps Pro exam:

1. [AWS CloudFormation](#)
2. [AWS Lambda](#)
3. [Amazon CloudWatch](#)
4. [Amazon EventBridge](#)
5. [Amazon CloudWatch Alarms](#)
6. [AWS CodePipeline](#)
7. [AWS CodeDeploy](#)
8. [AWS CodeBuild](#)
9. [AWS Config](#)
10. [AWS Systems Manager](#)
11. [Amazon ECS](#)
12. [Amazon Elastic Beanstalk](#)
13. [AWS CloudTrail](#)
14. [AWS Trusted Advisor](#)

The FAQs provide a good summary for each service, however, the AWS documentation contains more detailed information that you'll need to study. These details will be the deciding factor in determining the correct choice from the incorrect choices in your exam. To supplement your review of the services, we recommend that you take a look at [Tutorials Dojo's AWS Cheat Sheets](#). Their contents are well-written and straight to the point, which will help reduce the time spent going through FAQs and documentation.



Common Exam Scenarios

Scenario	Solution
Software Development and Lifecycle (SDLC) Automation	
An Elastic Beanstalk application must not have any downtime during deployment and requires an easy rollback to the previous version if an issue occurs.	Set up Blue/Green deployment, deploy a new version on a separate environment then swap environment URLs on Elastic Beanstalk.
A new version of an AWS Lambda application is ready to be deployed, and the deployment should not cause any downtime. A quick rollback to the previous Lambda version must be available.	Publish a new version of the Lambda function. After testing, use the production Lambda Alias to point to this new version.
In an AWS Lambda application deployment, only 10% of the incoming traffic should be routed to the new version to verify the changes before eventually allowing all production traffic.	Set up Canary deployment for AWS Lambda. Create a Lambda Alias pointed to the new Version. Set Weighted Alias value for this Alias as 10%.
An application hosted in Amazon EC2 instances behind an Application Load Balancer. You must provide a safe way to upgrade the version on Production and allow easy rollback to the previous version.	Launch the application in Amazon EC2 that runs the new version with an Application Load Balancer (ALB) in front. Use Route 53 to change the ALB A-record Alias to the new ALB URL. Rollback by changing the A-record Alias to the old ALB.
During the deployment, you need to run custom actions before deploying the new version of the application using AWS CodeDeploy.	Add lifecycle hook action BeforeAllowTraffic
You need to run custom verification actions after the new version is deployed using AWS CodeDeploy.	Add lifecycle hook action AfterAllowTraffic
You need to set up AWS CodeBuild to automatically run after a pull request has been successfully merged.	Create Amazon EventBridge rule to detect pull requests and action set to trigger CodeBuild Project. Use AWS Lambda to update the pull request with the result of the project Build



You need to use AWS CodeBuild to create artifact and automatically deploy the new application version	Set CodeBuild to save artifact to S3 bucket. Use CodePipeline to deploy using CodeDeploy and set the build artifact from the CodeBuild output.
You need to upload the AWS CodeBuild artifact to Amazon S3	S3 bucket needs to have versioning and encryption enabled.
You need to review AWS CodeBuild Logs and have an alarm notification for build results on Slack	Send AWS CodeBuild logs to CloudWatch Log group. Create Amazon EventBridge rule to detect the result of your build and target a Lambda function to send results to the Slack channel (or SNS notification)
Need to get a Slack notification for the status of the application deployments on AWS CodeDeploy	Create Amazon EventBridge rule to detect the result of CodeDeploy job and target a notification to Amazon SNS or a Lambda function to send results to Slack channel
Need to run an AWS CodePipeline every day for updating the development progress status	Create Amazon EventBridge rule to run on schedule every day and set a target to the AWS CodePipeline ARN
Automate deployment of a Lambda function and test for only 10% of traffic for 10 minutes before allowing 100% traffic flow.	Use CodeDeploy and select deployment configuration CodeDeployDefault.LambdaCanary10Percent10M inutes
Deployment of Elastic Beanstalk application with absolutely no downtime. The solution must maintain full compute capacity during deployment to avoid service degradation.	Choose the "Rolling with additional Batch" deployment policy in Elastic Beanstalk
Deployment of Elastic Beanstalk application where the new version must not be mixed with the current version.	Choose the "Immutable deployments" deployment policy in Elastic Beanstalk
Configuration Management and Infrastructure-as-Code (IaC)	
The resources on the parent CloudFormation stack needs to be referenced by other nested CloudFormation stacks	Use Export on the Output field of the main CloudFormation stack and use Fn::ImportValue function to import the value on the other stacks



On which part of the CloudFormation template should you define the artifact zip file on the S3 bucket?	The artifact file is defined on the AWS::Lambda::Function code resource block
Need to define the AWS Lambda function inline in the CloudFormation template	On the AWS::Lambda::Function code resource block, the inline function must be enclosed inside the ZipFile section.
Use CloudFormation to update Auto Scaling Group and only terminate the old instances when the newly launched instances become fully operational	Set AutoScalingReplacingUpdate : WillReplace property to TRUE to have CloudFormation retain the old ASG until the instances on the new ASG are healthy.
You can scale down the EC2 instances at night when there is low traffic using AWS Auto Scaling and Scheduled Scaling.	Create <i>Time-based</i> instances for automatic scaling of predictable workload.
Can't install an agent on on-premises servers but need to collect information for migration	Deploy the Agentless Discovery Connector VM on your on-premises data center to collect information.
Syntax for CloudFormation with an Amazon ECS cluster with ALB	Use the AWS::ECS::Service element for the ECS Cluster, AWS::ECS::TaskDefinition element for the ECS Task Definitions, and the AWS::ElasticLoadBalancingV2::LoadBalancer element for the ALB.
Monitoring and Logging	
Need to centralize audit and collect configuration settings on all regions of multiple accounts	Setup an Aggregator on AWS Config.
Consolidate CloudTrail log files from multiple AWS accounts	Create a central S3 bucket with bucket policy to grant cross-account permission. Set this as destination bucket on the CloudTrail of the other AWS accounts.
Ensure that CloudTrail logs on the S3 bucket are protected and cannot be tampered with.	Enable Log File Validation on CloudTrail settings



Need to collect/investigate application logs from EC2 or on-premises server	Install CloudWatch Logs Agent to send the logs to CloudWatch Logs for storage and viewing.
Need to review logs from running ECS Fargate tasks	Enable awslogs log driver on the Task Definition and add the required logConfiguration parameter.
Need to run real-time analysis for collected application logs	Send logs to CloudWatch Logs, create a Lambda subscription filter, OpenSearch subscription filter, or Kinesis stream filter.
Need to be automatically notified if you are reaching the limit of running EC2 instances or limit of Auto Scaling Groups	Track service limits with Trusted Advisor on CloudWatch Alarms using the ServiceLimitUsage metric.
Security and Compliance	
Need to secure the buildspec.yml file, which contains the AWS keys and database password stored in plaintext.	Store these values as encrypted parameter on SSM Parameter Store
You need to secure an S3 bucket by ensuring that only HTTPS requests are allowed for compliance purposes.	Create an S3 bucket policy that Deny if checks for condition aws:SecureTransport is false
Need to store a secret, database password, or variable, in the most cost-effective solution	Store the variable on SSM Parameter Store and enable encryption
Need to generate a secret password and have it rotated automatically at regular intervals	Store the secret on AWS Secrets Manager and enable key rotation.
Several team members with designated roles need to be granted permission to use AWS resources	Assign AWS-managed policies on the IAM accounts such as, ReadOnlyAccess, AdministratorAccess, PowerUserAccess
Apply latest patches on EC2 and automatically create an AMI	Use Systems Manager automation to execute an Automation Document that installs OS patches and creates a new AMI.
Need to have a secure SSH connection to EC2 instances and have a record of all commands executed during the session	Install SSM Agent on EC2 and use SSM Session Manager for the SSH access. Send the session logs to S3 bucket or CloudWatch Logs for auditing and review.



Ensure that the managed EC2 instances have the correct application version and patches installed.	Use SSM Inventory to have visibility of your managed instances and identify their current configurations.
Apply custom patch baseline from a custom repository, and schedule patches to managed instances	Use SSM Patch Manager to define a custom patch baseline and schedule the application patches using SSM Maintenance Windows
Incident and Event Response	
Need to get a notification if somebody deletes files in your S3 bucket	Setup Amazon S3 Event Notifications to get notifications based on specified S3 events on a particular bucket.
Need to be notified when an RDS Multi-AZ failover happens	Setup Amazon RDS Event Notifications to detect specific events on RDS.
Get a notification if somebody uploaded IAM access keys on any public GitHub repositories	Create an Amazon EventBridge rule for the AWS_RISK_CREDENTIALS_EXPOSED event from AWS Health Service. Use AWS Step Functions to automatically delete the IAM key.
Get notified on Slack when your EC2 instance is having an AWS-initiated maintenance event	Create an Amazon EventBridge rule for the AWS Health Service to detect EC2 Events. Target a Lambda function that will send a notification to the Slack channel
Get notified of any AWS maintenance or events that may impact your EC2 or RDS instances	Create an Amazon EventBridge rule for detecting any events on AWS Health Service and send a message to an SNS topic or invoke a Lambda function.
Monitor scaling events of your Amazon EC2 Auto Scaling Group, such as launching or terminating an EC2 instance.	Use Amazon EventBridge for monitoring the Auto Scaling Service and monitor the EC2 Instance-Launch Successful and EC2 Instance-Terminate Successful events.
View object-level actions of S3 buckets, such as upload or deletion of object in CloudTrail	Set up Data events on your CloudTrail trail to record object-level API activity on your S3 buckets.