AWS CERTIFIED
DevOps Engineer Pro

# DOP-C02

DevOps Engineer Professional
QUICK REFERENCE

| 75 Questions | 180 Min | 750/1000 to Pass | 6 Domains | No Penalty Guessing |
|---|---|---|---|---|

| D1 SDLC Automation 22% | D2 Config Mgmt & IaC 17% | D3 Resilient Solutions 15% | D4 Monitoring & Logs 15% | D5 Incident Response 14% | D6 Security & Compliance 17% |
|---|---|---|---|---|---|

## DOMAIN 1 SDLC AUTOMATION 22%

- **CodePipeline:** Orchestrates Source-Build-Test-Deploy; Manual Approval action; cross-account/region actions; EventBridge on state changes
- **buildspec.yml phases:** install, pre_build, build, post_build; reports section for test results; artifacts block uploads to S3
- **CodeBuild VPC:** Specify VPC ID + subnet + SG to reach private resources (RDS, ElastiCache)
- **CodeDeploy EC2 hooks:** ApplicationStop, DownloadBundle, BeforeInstall, Install, AfterInstall, ApplicationStart, ValidateService
- **CodeDeploy Lambda hooks:** BeforeAllowTraffic, AllowTraffic, AfterAllowTraffic
- **ECS Blue/Green:** New task set; ALB listener shifts; test listener for validation; old task set decommissioned after bake period
- **Canary10Percent5Minutes:** 10% to new Lambda version, wait 5 min, then 100%; CW alarm triggers auto-rollback
- **CodeArtifact:** Private repo for npm/Maven/pip/NuGet; upstream caching from public registries; domain contains repos
- **EC2 Image Builder:** Automates golden AMI creation, patching, testing, distribution to regions/accounts
- **EB Immutable deploy:** New ASG with new version; health checked before traffic; rollback = terminate new ASG instantly
- **SSM SecureString in buildspec:** Reference via parameter-store section; values masked in logs; KMS decryption required

| Strategy | Traffic Shift | Rollback Trigger |
|---|---|---|
| Canary10Pct5Min | 10% wait 5min then 100% | CW Alarm |
| Linear10PctEvery1Min | +10% every minute | CW Alarm |
| AllAtOnce | Instant 100% | Deploy failure |
| Blue/Green (ECS) | ALB listener swap | Manual or alarm |

## DOMAIN 3 RESILIENT CLOUD SOLUTIONS 15%

- **ASG Warm Pools:** Pre-initialized stopped instances; scale-out in seconds vs minutes; pay EBS costs only; configure pool min/max size
- **ASG Lifecycle Hooks:** Terminating:Wait lets Lambda drain connections; call CompleteLifecycleAction to proceed; Pending:Wait for scale-out
- **Target Tracking Scaling:** Maintain metric at target; ScaleInCooldown / ScaleOutCooldown; DisableScaleIn option available
- **SQS Standard vs FIFO:** Standard = at-least-once, best-effort order, unlimited TPS; FIFO = exactly-once, strict order, 3,000 TPS
- **SQS DLQ:** Receives messages after maxReceiveCount failures; prevents poison pills; set long retention for investigation and replay
- **Lambda + SQS retries:** Set maxReceiveCount on SOURCE SQS queue (not Lambda DLQ); Lambda DLQ = async invocations only
- **SQS backlog per instance:** ApproximateNumberOfMessagesVisible / InService instances; publish as custom CW metric for ASG scaling
- **ALB cross-zone LB:** Default enabled on ALB; distributes to healthy targets in all AZs; failed AZ targets removed automatically
- **Aurora Global DB:** RPO less than 1s; RTO approx 1 min managed planned failover; secondary promoted; requires DNS update
- **Lambda async retries:** Max retry attempts (0-2) + Max event age (60s to 6hr); expired events go to DLQ or Failure Destination

| DR Strategy | RTO | RPO | Cost |
|---|---|---|---|
| Backup & Restore | Hours | Hours | Lowest |
| Pilot Light | 30 min | Minutes | Low |
| Warm Standby | ~15 min | Seconds | Medium |
| Multi-Site Active | Near 0 | Near 0 | Highest |

## DOMAIN 2 CONFIG MGMT & IaC 17%

- **StackSets SERVICE_MANAGED:** Organizations auto-deploy to OU; new accounts auto-get stack; accounts leaving OU optionally cleaned
- **StackSets SELF_MANAGED:** Manually specify target account IDs; requires cross-account IAM roles
- **cfn-signal + CreationPolicy:** EC2 user data signals CloudFormation on bootstrap completion; prevents premature stack creation success
- **DeletionPolicy Snapshot:** Final RDS snapshot before deletion; Retain = keep resource running; Delete = destroy (default)
- **Cross-stack references:** Export values with Export:Name in Outputs; consume with Fn::ImportValue; dependency enforced by CFn
- **CFn Drift Detection:** Compares live config vs template; detect-stack-drift API; schedule via EventBridge + Lambda for continuous monitoring
- **CAPABILITY_NAMED_IAM:** Required when template creates IAM resources with custom names; CAPABILITY_IAM = auto-named only
- **SSM State Manager:** Continuously enforces desired config via scheduled associations; corrects configuration drift automatically
- **Config Conformance Pack:** Bundle of Config rules + remediation; prebuilt packs for CIS/PCI/HIPAA; org-level deployment via delegated admin
- **SSM Automation rate control:** MaxConcurrency = parallel targets; MaxErrors = stop threshold; critical for large-scale safe runbook execution
- **.ebextensions:** YAML files in app bundle; option_settings, packages, files, commands, container_commands per environment

| Feature | SSM Parameter Store | Secrets Manager |
|---|---|---|
| Cost | Free std / $0.05 advanced | $0.40/secret/month |
| Auto Rotation | No | Yes - RDS, Redshift, DocDB |
| KMS | SecureString type | Always encrypted |
| Best For | Config, non-secret strings | Credentials, API keys |

## DOMAIN 4 MONITORING & LOGGING 15%

- **CloudWatch Agent:** Collects memory, disk, swap (not in default EC2 metrics); deploy via SSM Run Command; JSON config
- **Embedded Metrics Format (EMF):** Structured JSON to Lambda stdout; CW asynchronously extracts metrics; no PutMetricData API latency
- **Composite Alarm:** AND/OR/NOT logic on multiple alarms; fires only when AlarmRule evaluates true; reduces notification noise
- **CloudWatch Logs Insights:** SQL-like queries across multiple log groups simultaneously; filter/stats/sort/limit for ad-hoc investigation
- **Metric Filters:** Pattern match on log events, increment custom CW metric, drive alarms; test pattern against sample events first
- **CloudTrail Data Events:** S3 object ops, Lambda invocations, DynamoDB item calls; opt-in; needed for forensic data access investigation
- **CloudTrail Log File Integrity:** Hourly SHA-256 digest files chained together; validate-logs proves no tampering for auditors
- **CloudTrail Insights:** ML baseline on write API rates; detects unusual spikes (credential abuse, resource bursts); publishes to EventBridge
- **X-Ray Annotations vs Metadata:** Annotations = indexed, filterable; Metadata = not indexed, arbitrary; X-Ray Daemon batches on UDP 2000
- **Treat missing data = breaching:** Alarm enters ALARM if metric stops reporting; use for health-check metrics where silence = problem
- **Cross-account log centralization:** CW Logs subscription filter to Kinesis Firehose destination in central account to S3 for archival

| Tool | Purpose | Key Fact |
|---|---|---|
| CloudWatch Agent | OS metrics (mem/disk) | Must install; deploy via SSM |
| EMF | Lambda custom metrics | No PutMetricData API call |
| X-Ray | Distributed tracing | Annotations indexed; metadata not |
| CloudTrail Insights | API anomaly detection | ML baseline on write API rates |

## DOMAIN 5 INCIDENT & EVENT RESPONSE 14%

- **GuardDuty auto-remediation:** Finding, EventBridge, Lambda: deny-all SG + EBS snapshot + notify SNS; do NOT delete instance (preserves evidence)
- **Config auto-remediation:** NON_COMPLIANT triggers SSM Automation doc; parameter mapping from Config evaluation; retry count configurable
- **Auto-tagging at launch:** EventBridge rule on EC2:RunInstances via CloudTrail, Lambda, ec2:CreateTags within seconds of launch
- **SSM Automation multi-step:** Steps reference previous outputs via {{StepName.OutputKey}}; supports rate control + cross-account execution
- **EventBridge tag filtering:** Tags NOT in state-change events; EventBridge to Lambda to DescribeTags to conditional action based on tag
- **CodeDeploy alarm rollback:** Associate CW alarm with deployment group rollback triggers; fires automatically on error rate spike
- **Config Aggregator:** Centralize compliance data from all org accounts; org integration auto-includes new accounts added later
- **SSM multi-account automation:** Specify account list + regions; SSM assumes execution role per account; MaxConcurrency controls parallelism
- **Inspector to quarantine:** Inspector CRITICAL finding, EventBridge rule, Lambda, deny-all SG applied + SOC notification sent
- **AWS Health to EventBridge:** Automate response to maintenance/retirement events; Lambda can schedule T-48h pre-action workflow

| Pattern | Trigger | Action |
|---|---|---|
| Auto-tagging | EC2 RunInstances event | Lambda calls CreateTags |
| GuardDuty remediate | Finding in EventBridge | Deny-all SG + EBS snapshot |
| Config fix | NON_COMPLIANT eval | SSM Automation runbook |
| Inspector quarantine | CRITICAL finding | Deny-all SG + notify |

## DOMAIN 6 SECURITY & COMPLIANCE 17%

- **Secrets Manager in Lambda:** GetSecretValue + Lambda extension caching with TTL; auto-rotation built-in for RDS/Aurora/Redshift
- **Rotation phases:** createSecret (AWSPENDING), setSecret (update service), testSecret (verify connectivity), finishSecret (promote to AWSCURRENT)
- **IAM DB Auth:** Short-lived token (15 min) via rds:connect IAM permission; eliminates password management; SSL/TLS required
- **Permission Boundaries:** Cap max perms for specific IAM entity; effective = intersection of identity policy AND boundary; safe delegation
- **SCPs vs Boundaries:** SCP = max perms for entire AWS account or OU; Boundary = max perms for specific IAM user or role
- **KMS Envelope Encryption:** GenerateDataKey, encrypt data locally, store encrypted data key with ciphertext; CMK never leaves KMS
- **CloudHSM:** Single-tenant FIPS 140-2 Level 3; only you control key material; use when regulations require exclusive key control
- **Macie:** S3 sensitive data discovery (PII, credit cards, API keys); monitors bucket ACLs; findings to EventBridge + Security Hub
- **WAF rate-based rule:** Auto-block IPs exceeding threshold in 5-min window; auto-unblock when rate drops; fully automated in WAF
- **SCP for RDS encryption:** Deny rds:CreateDBInstance when StorageEncrypted is false; preventive control; even admins cannot bypass
- **GuardDuty sources:** VPC Flow Logs + CloudTrail + DNS always on; optional: EKS audit logs, S3 data events, RDS login, Lambda network
- **Security Hub:** Aggregates GuardDuty/Macie/Inspector/Config in ASFF format; org delegated admin sees all accounts; CIS/PCI standards

| Control Type | Service | Key Fact |
|---|---|---|
| Preventive | SCP | Deny at account/OU level; before action |
| Preventive | Permission Boundary | Cap max perms per IAM entity |
| Detective | GuardDuty | ML on VPC Flow Logs + CloudTrail + DNS |
| Detective | Macie | PII discovery in S3; monitors bucket ACLs |
| Responsive | EventBridge + Lambda | Automated remediation on findings |

## MASTER QUICK REFERENCE — KNOW THESE COLD

| Service / Concept | Dom | The Key Fact to Remember |
|---|---|---|
| **Canary10Percent5Minutes** | D1 | 10% to new Lambda version, wait 5 min, then 100%; CW alarm triggers rollback during bake |
| **CodeBuild buildspec.yml** | D1 | Phases: install, pre_build, build, post_build; reports block for test results; artifacts block to S3 |
| **CodeDeploy EC2 appspec hooks** | D1 | ApplicationStop, DownloadBundle, BeforeInstall, Install, AfterInstall, ApplicationStart, ValidateService |
| **ECS Blue/Green (CodeDeploy)** | D1 | New task set created; ALB listener shifts after health check; old task set decommissioned post-bake |
| **EB Immutable Deployment** | D1 | New ASG with new version; health checked before any traffic shift; rollback = terminate new ASG instantly |
| **CodeBuild VPC access** | D1 | Configure project with VPC ID + subnet IDs + SG; target SG must allow inbound from CodeBuild SG |
| **StackSets SERVICE_MANAGED** | D2 | Uses Organizations; auto-deploys to new accounts joining OU; optional cleanup when accounts leave OU |
| **cfn-signal + CreationPolicy** | D2 | User data calls cfn-signal on success/failure; CFn waits for ResourceSignal count before stack proceeds |
| **DeletionPolicy Snapshot** | D2 | Final RDS snapshot before deletion; Retain = keep resource running; Delete = destroy (default) |
| **SSM State Manager** | D2 | Scheduled associations enforce desired config continuously; corrects drift on next run automatically |
| **Config Conformance Pack** | D2 | Bundle of rules + remediation; prebuilt CIS/PCI/HIPAA; deploy org-wide from delegated admin account |
| **SSM Automation MaxConcurrency** | D2 | Limits parallel targets; MaxErrors stops automation at failure threshold; safe large-scale execution |
| **ASG Warm Pools** | D3 | Pre-initialized stopped instances; scale-out in seconds vs minutes; pay EBS only; configure pool size |
| **ASG Lifecycle Hook Terminating** | D3 | Instance enters Terminating:Wait; Lambda drains connections; CompleteLifecycleAction resumes termination |
| **SQS DLQ maxReceiveCount** | D3 | After N failed deliveries, message goes to DLQ; for Lambda+SQS configure on source queue not Lambda DLQ |
| **SQS backlog per instance metric** | D3 | ApproximateNumberOfMessagesVisible / InService instances; custom CW metric for ASG target tracking policy |
| **Aurora Global DB failover** | D3 | RPO less than 1 second; RTO approx 1 min managed planned failover; secondary promoted; update DNS |
| **CloudWatch Agent** | D4 | Required for memory, disk, swap metrics; not in default EC2 metrics; deploy via SSM Run Command at scale |
| **Embedded Metrics Format EMF** | D4 | Structured JSON to Lambda stdout; CW asynchronously extracts metrics; no PutMetricData API or latency |
| **Composite Alarm** | D4 | AND/OR/NOT logic on multiple alarms; fires only when AlarmRule is true; reduces alert noise significantly |
| **CloudTrail Data Events** | D4 | S3 object ops, Lambda invocations, DynamoDB item calls; opt-in; essential for forensic data access investigation |
| **CloudTrail Log Integrity** | D4 | Hourly SHA-256 digest files chained together; validate-logs proves no tampering for audit compliance |
| **X-Ray Annotations** | D4 | Indexed key-value pairs for search and filter; Metadata = not indexed; X-Ray Daemon batches traces on UDP 2000 |
| **Treat Missing Data breaching** | D4 | Alarm enters ALARM if metric stops reporting; use for health-check style metrics where silence equals problem |
| **GuardDuty auto-remediation** | D5 | Finding to EventBridge to Lambda: deny-all SG isolation + EBS snapshot + SNS notify; never delete instance |
| **Config auto-remediation** | D5 | NON_COMPLIANT triggers SSM Automation document; parameter mapping from Config evaluation result |
| **EventBridge tag filtering** | D5 | Tags NOT in state-change events; EventBridge to Lambda to DescribeTags to conditional action on tag value |
| **CodeDeploy alarm rollback** | D5 | Associate CW alarm with deployment group rollback triggers; fires automatically on error rate spike |
| **SSM multi-account automation** | D5 | Specify account list and regions; SSM assumes execution role per account; MaxConcurrency controls parallelism |
| **Secrets Manager rotation** | D6 | 3-phase Lambda: createSecret (AWSPENDING), setSecret, testSecret, finishSecret (promotes to AWSCURRENT) |
| **IAM Database Auth** | D6 | Short-lived token 15 min via rds:connect permission; no password management; SSL required; MySQL/Postgres/Aurora |
| **Permission Boundaries** | D6 | Cap max perms for specific IAM entity; effective = intersection of identity policy AND boundary; safe delegation |
| **KMS Envelope Encryption** | D6 | GenerateDataKey, encrypt data locally, store encrypted data key with ciphertext; CMK never leaves KMS |
| **CloudHSM** | D6 | Single-tenant FIPS 140-2 Level 3; only you control key material; use when regulations require exclusive control |
| **WAF rate-based rule** | D6 | Auto-block IPs exceeding threshold in 5-min window; auto-unblock when rate drops; fully automated in WAF |
| **SCP encryption enforcement** | D6 | Deny rds:CreateDBInstance when StorageEncrypted is false; preventive control; even account admins cannot bypass |
| **Security Hub** | D6 | Aggregates GuardDuty/Macie/Inspector/Config in ASFF; org delegated admin sees all accounts; CIS/PCI standards |

| | | |
|---|---|---|
| **EXAM TIPS: 750/1000 to pass \| 75 Qs \| 180 min \| No penalty for guessing \| Mark and review unknown Qs** | **HOT TOPICS: Canary Lambda \| cfn-signal CreationPolicy \| SQS DLQ for Lambda \| Secrets Manager rotation phases \| Warm Pools** | **ALWAYS: EMF over PutMetricData \| Warm Pools fast scale \| CloudTrail data events for forensics \| SCP prevents, Config detects** |