# AWS Certified DevOps Engineer - Professional Cheat Sheet

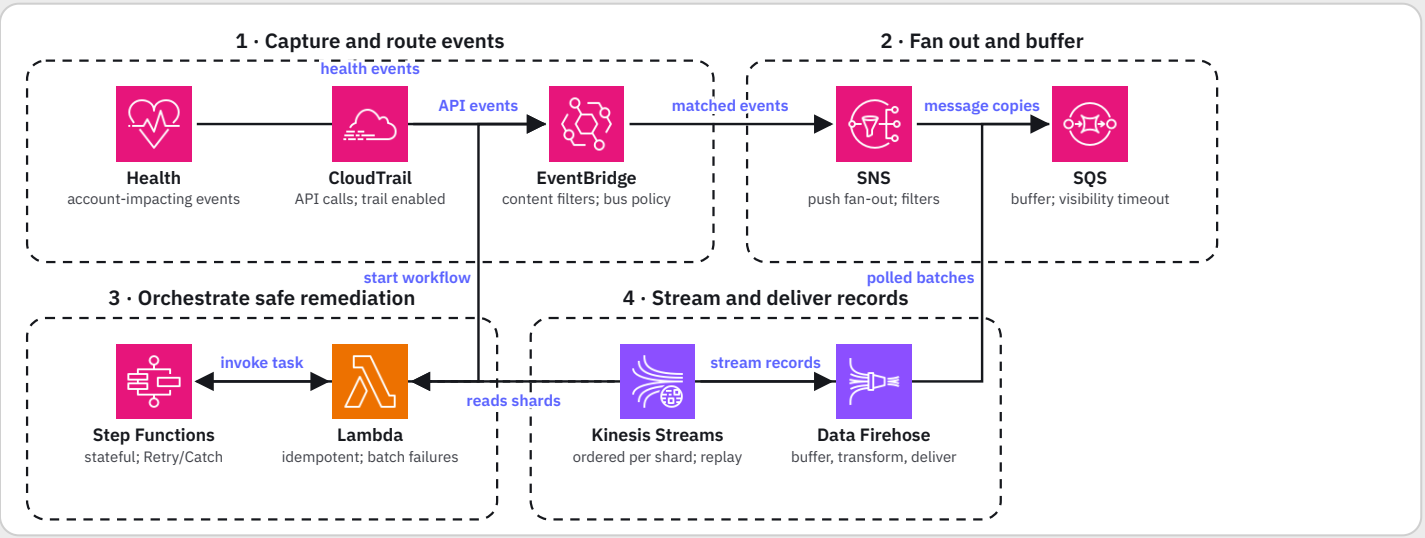
DOP-C02 · Domain 5 of 6

BlowStack

DOMAIN 5 · INCIDENT AND EVENT RESPONSE · 14% OF THE EXAM · TASK STATEMENT 5.1

## Manage event sources to process, notify, and take action in response to events

### Route, buffer, orchestrate, stream




**1 Capture and route events**

Use **event patterns** for content-based routing. CloudTrail-backed API events require trail logging. Cross-account delivery needs a destination bus policy and an authorized sender role.

**2 Fan out and buffer**

Use **SNS-to-SQS fan-out** for independent, buffered consumers. SNS pushes copies; SQS consumers poll. Visibility timeout hides work temporarily; successful processing must delete the message.

**3 Orchestrate safe remediation**

Use **Step Functions** for stateful branching, waits, Retry and Catch; Lambda runs remediation code. For SQS-triggered Lambda, enable partial batch responses and make actions idempotent.

**4 Stream and deliver records**

Choose **replayable streams** for independent consumers and retained records. Kinesis consumers track their positions; Firehose buffers and delivers to destinations rather than orchestrating remediation.

### Exam traps

- An **EventBridge target DLQ** captures exhausted delivery failures, not a target's later processing errors. Consumer failures need queue redrive or workflow error handling.
- A **visibility timeout** is not deletion or exactly-once delivery. Standard queues can redeliver; allow enough processing time and use idempotent consumers.
- **Amazon Kinesis Data Streams** supports replay and per-shard ordering. Amazon Data Firehose buffers delivery, not arbitrary consumer replay. Neither provides work-queue semantics.

Get practice exams and lessons for AWS Certified DevOps Engineer - Professional

# AWS Certified DevOps Engineer - Professional Cheat Sheet

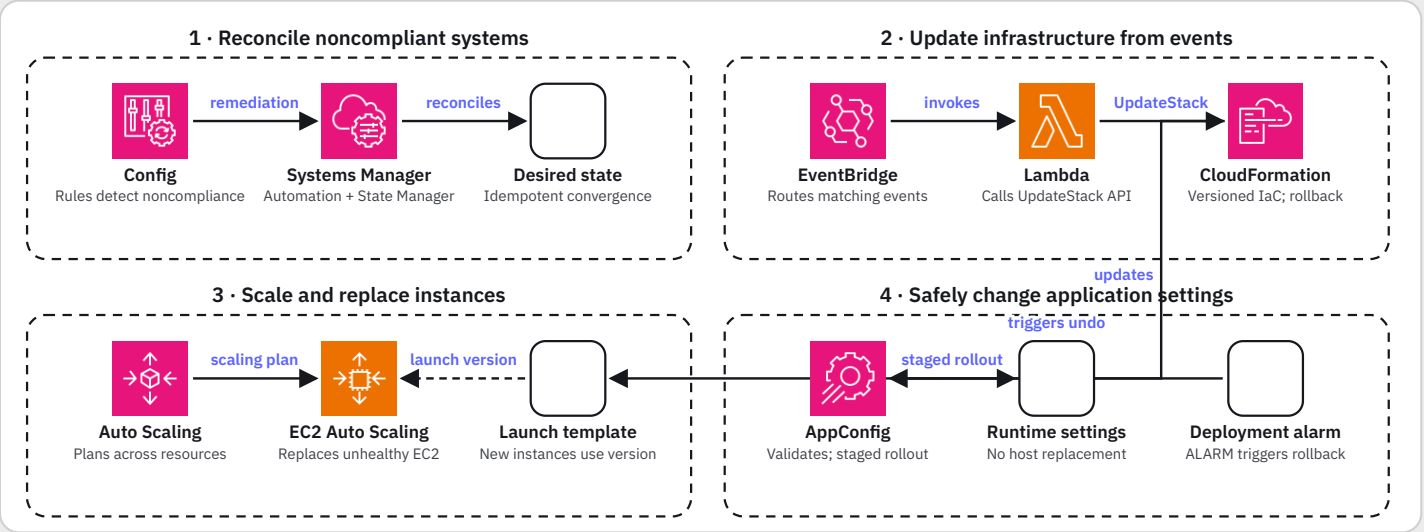
DOP-C02 · Domain 5 of 6

BlowStack

DOMAIN 5 · INCIDENT AND EVENT RESPONSE · TASK STATEMENT 5.2

## Implement configuration changes in response to events

### Detect, remediate, update, roll back




### 1 Reconcile noncompliant systems

**Automation remediation** runs runbooks for Config noncompliance; State Manager associations periodically reapply desired state. AWS Config evaluates resources; it does not change them itself.

### 2 Update infrastructure from events

For **event-driven IaC**, EventBridge invokes Lambda to call CloudFormation UpdateStack. Templates remain the source of truth; failed stack updates can roll back.

### 3 Scale and replace instances

AWS Auto Scaling builds scaling plans; **instance refresh** rolls existing EC2 instances to a new launch template version. Template edits alone do not update running instances.

### 4 Safely change application settings

**Application settings** use AppConfig validators and gradual deployment; configured alarms can automatically roll back a bad release. OS configuration uses Systems Manager, not AppConfig.

## Exam traps

- **Drift detection is not repair**: AWS Config evaluates compliance; CloudFormation drift detection reports differences. Detection alone does not restore desired state.
- **At-least-once events** can repeat; Lambda handlers and remediation runbooks must be idempotent. Automatic retries do not make changes safe to repeat.
- AWS OpsWorks is **retired**, not a new-workload choice; support ended May 1, 2024. AWS Systems Manager supports ongoing OS configuration management.

Get practice exams and lessons for AWS Certified DevOps Engineer - Professional

# AWS Certified DevOps Engineer - Professional Cheat Sheet

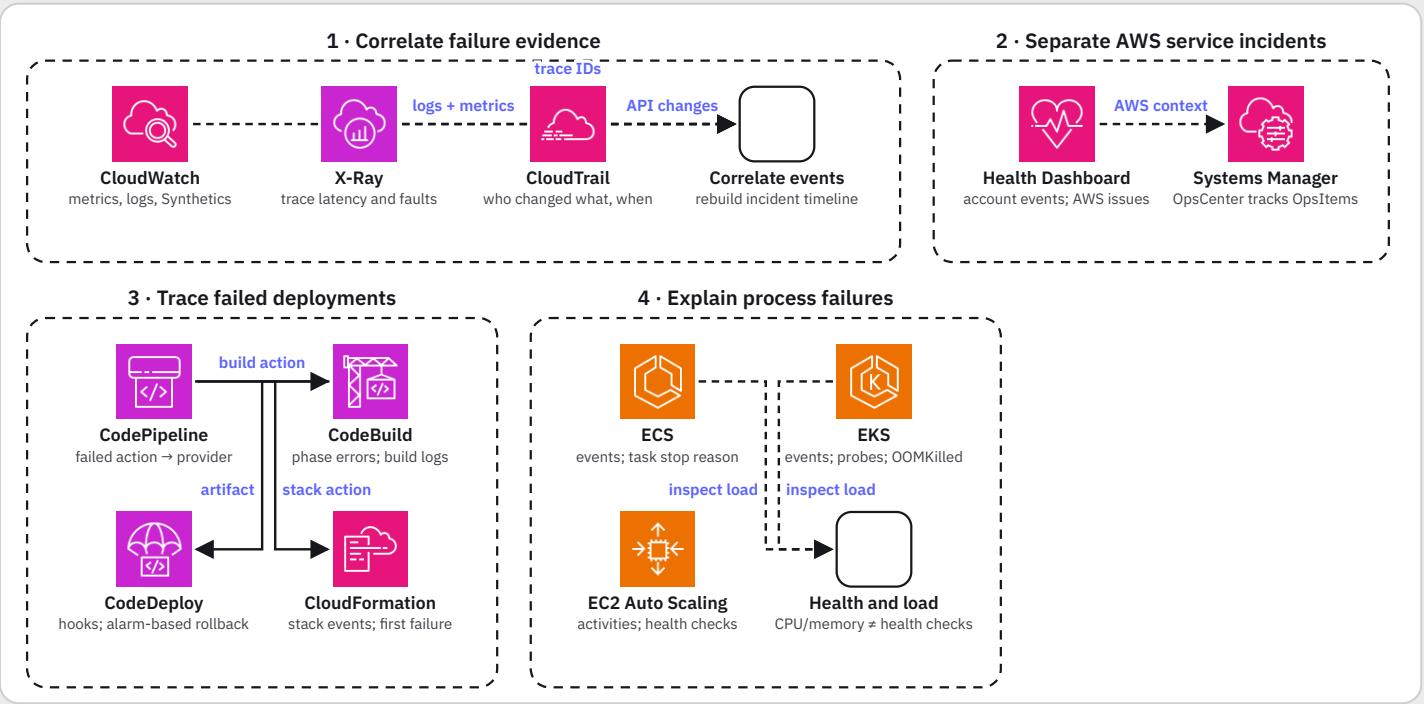
DOP-C02 · Domain 5 of 6

BlowStack

DOMAIN 5 · INCIDENT AND EVENT RESPONSE · TASK STATEMENT 5.3

## Troubleshoot system and application failures

### Observe, correlate, inspect, recover




#### 1 Correlate failure evidence

**Root cause** needs a timeline: correlate timestamps, resource IDs, request IDs, and API changes. CloudWatch exposes symptoms; X-Ray localizes traced latency; CloudTrail identifies the change actor.

#### 2 Separate AWS service incidents

For an **AWS-side incident**, check account-specific Health events before changing workloads. OpsCenter centralizes OpsItems and investigation context; remediation requires configured Automation, not merely an open OpsItem.

#### 3 Trace failed deployments

At a **failed action**, inspect provider logs or stack events. CodeDeploy automatic rollback must be enabled and deploys a previous revision; CloudFormation rollback restores stack state, not application data.

#### 4 Explain process failures

For **unhealthy workloads**, inspect task/pod events and scaling activities before adding capacity. Auto Scaling replaces unhealthy instances; load-balancer health must be enabled. High utilization alone is not failed health.

### Exam traps

- **CloudTrail is not an application log**: it records API activity. CloudWatch logs expose application errors; X-Ray requires tracing instrumentation to explain distributed request failures.
- **An alarm does not guarantee rollback**: CodeDeploy needs alarm monitoring and automatic rollback configured. A previous revision must remain deployable; rollback does not reverse database changes.
- **Readiness is not liveness**: failed readiness removes a pod from service traffic; failed liveness restarts its container. Adding capacity does not repair a broken probe or application defect.

Get practice exams and lessons for AWS Certified DevOps Engineer - Professional

# AWS Certified DevOps Engineer - Professional Cheat Sheet

DOP-C02 · Domain 5 of 6

BlowStack

DOMAIN 5 · INCIDENT AND EVENT RESPONSE · WHAT TO REMEMBER

## Concepts and services of Incident and Event Response

### Concepts to know

**Event-Driven Architecture**

Decouples producers from consumers through events. Choose **routing, buffering, or orchestration** according to whether the response needs selective delivery, backlog absorption, or coordinated steps with state and retries.

**Configuration Drift**

Running resources diverge from their intended configuration. Choose **detection plus controlled remediation** to restore desired state; compliance evaluation identifies violations, while remediation automation applies corrections.

**Event Correlation**

Connects metrics, logs, traces, API activity, and deployment events to explain failures. Use **time-aligned evidence** to distinguish a triggering change from downstream symptoms before choosing remediation or rollback.

### Core services



**Amazon EventBridge**

Choose **event-pattern rules** to route AWS service or custom events to response targets. Target retry policies and dead-letter queues handle delivery failures, not failures inside a target.



**AWS Systems Manager**

Choose **Automation runbooks** for coordinated remediation, Run Command for commands across managed nodes, and State Manager associations for maintaining desired configuration.



**Amazon CloudWatch**

Choose **metric alarms** for threshold-based response, Logs Insights to investigate application logs, and Synthetics canaries to detect endpoint or user-workflow failures.

Get practice exams and lessons for AWS Certified DevOps Engineer - Professional