AWS Certified DevOps Engineer - Professional Cheat Sheet

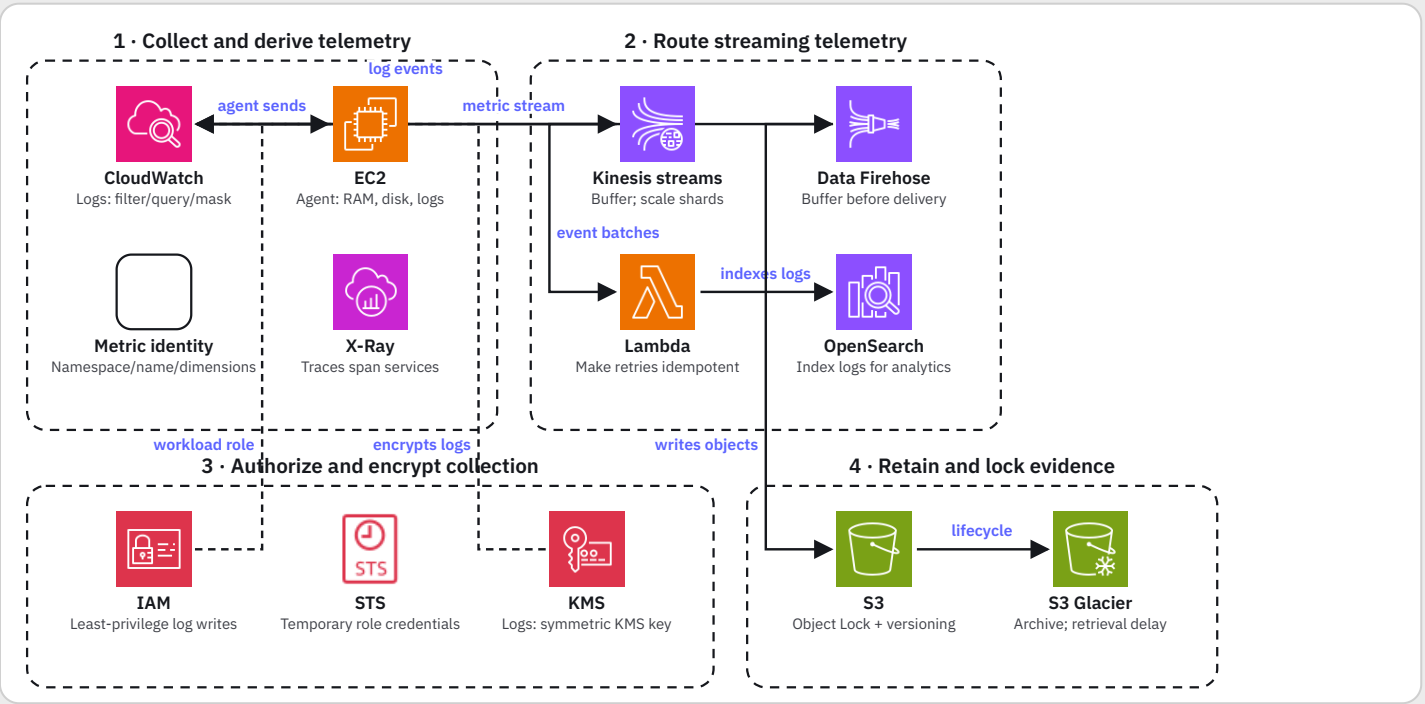
DOP-C02 · Domain 4 of 6

BlowStack

DOMAIN 4 · MONITORING AND LOGGING · 15% OF THE EXAM · TASK STATEMENT 4.1

Configure the collection, aggregation, and storage of logs and metrics

Collect, derive, route, protect, retain



1 Collect and derive telemetry

Use **metric filters** for persistent log-derived metrics; Logs Insights queries logs. Custom metrics support 1-second resolution versus standard 60 seconds. Each dimension combination creates a separate time series.

2 Route streaming telemetry

Metric streams deliver through Firehose, not directly to S3. Log subscriptions target Kinesis, Firehose, or Lambda. At-least-once delivery requires duplicate handling; monitor throttling and consumer lag.

3 Authorize and encrypt collection

Cross-account roles need caller permission and target trust. Workloads use temporary credentials. Log-write permission does not grant KMS access. TLS protects transit; server-side KMS encryption protects stored data.

4 Retain and lock evidence

Retention is explicit: CloudWatch Logs defaults to never expire. Set log-group retention; separately deliver logs to S3 for lifecycle tiering. Object Lock compliance mode prevents early deletion, even by root.

Exam traps

- **High resolution is not permanent**: sub-minute CloudWatch metric data lasts 3 hours; older data uses coarser aggregation. Choose periods and statistics that preserve the signal.
- **Client-side encryption** makes log contents unreadable to server-side filters and queries. TLS and server-side KMS encryption preserve service-side processing; masking separately limits exposure.
- **Retention is not archival**: CloudWatch Logs retention deletes events; it does not export them. Configure export or continuous delivery separately before relying on S3 lifecycle rules.

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

AWS Certified DevOps Engineer - Professional Cheat Sheet

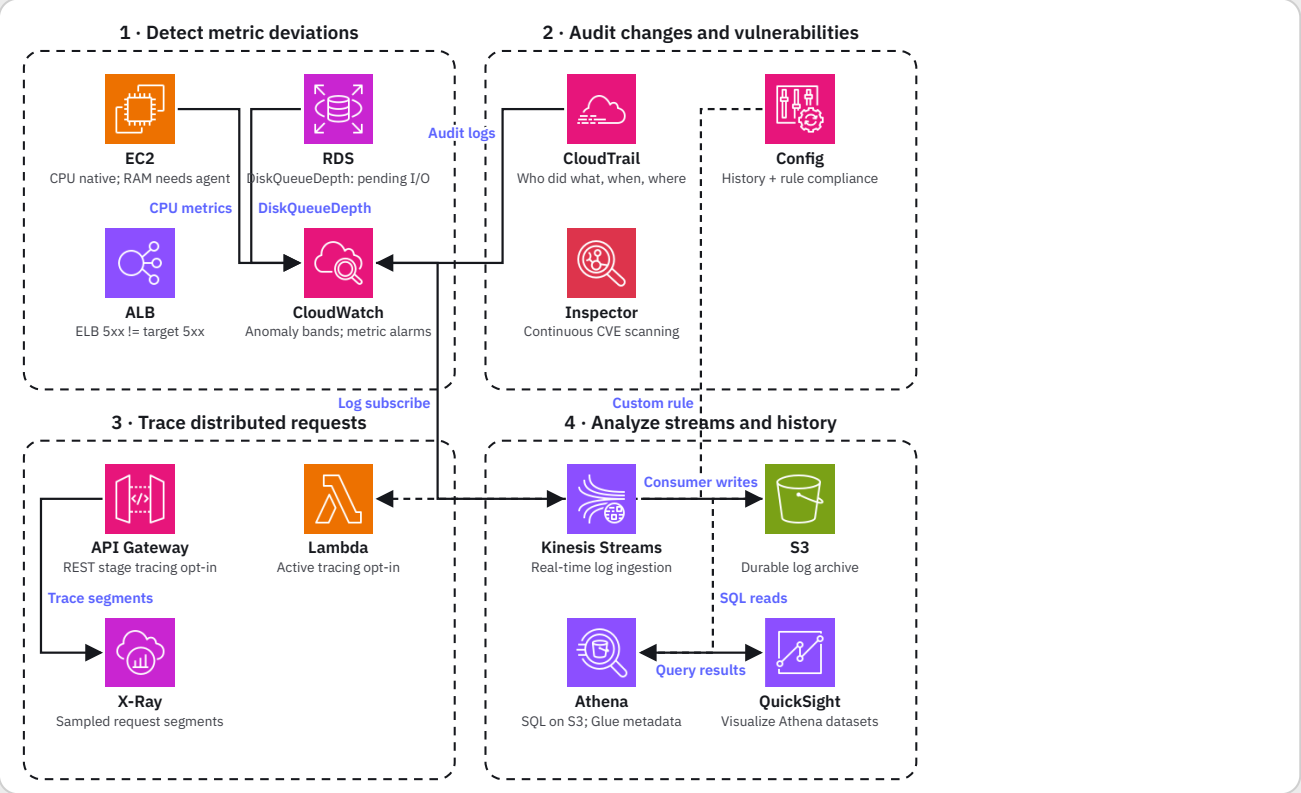
DOP-C02 · Domain 4 of 6

BlowStack

DOMAIN 4 · MONITORING AND LOGGING · TASK STATEMENT 4.2

Audit, monitor, and analyze logs and metrics to detect issues

Detect, audit, trace, analyze



1 Detect metric deviations

Unusual baseline: anomaly alarms compare metrics with learned bands. Standard or custom metrics can drive alarms and SNS actions; dashboards visualize metrics. EC2 basic monitoring is 5 minutes; detailed is 1 minute.

2 Audit changes and vulnerabilities

API activity: CloudTrail events match EventBridge rules; delivered CloudWatch logs support metric-filter alarms. Config evaluates recorded configuration using managed or custom rules; Inspector finds vulnerabilities.

3 Trace distributed requests

End-to-end traces require tracing on REST API stages and Lambda, plus application instrumentation and a collector for ECS/EKS. X-Ray samples requests; logs alone do not create distributed traces.

4 Analyze streams and history

For **real time**, Kinesis consumers use Lambda or Apache Flink. Logs Insights queries CloudWatch logs; Athena queries S3 using Glue metadata; QuickSight visualizes datasets; OpenSearch indexes searchable logs.

Exam traps

- **Assessment templates** belong to Inspector Classic, not current Inspector. Current EC2 scanning uses Systems Manager for agent-based scans or agentless scanning on eligible instances.
- **ALB 5xx metrics** distinguish load-balancer errors, HTTPCode_ELB_5XX_Count, from target errors, HTTPCode_Target_5XX_Count. An alarm on one does not detect errors counted only by the other.
- **CloudTrail Event history** covers 90 days of management events, not data events. Data-event auditing requires explicit selectors; durable retention requires a trail or event data store.

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

AWS Certified DevOps Engineer - Professional Cheat Sheet

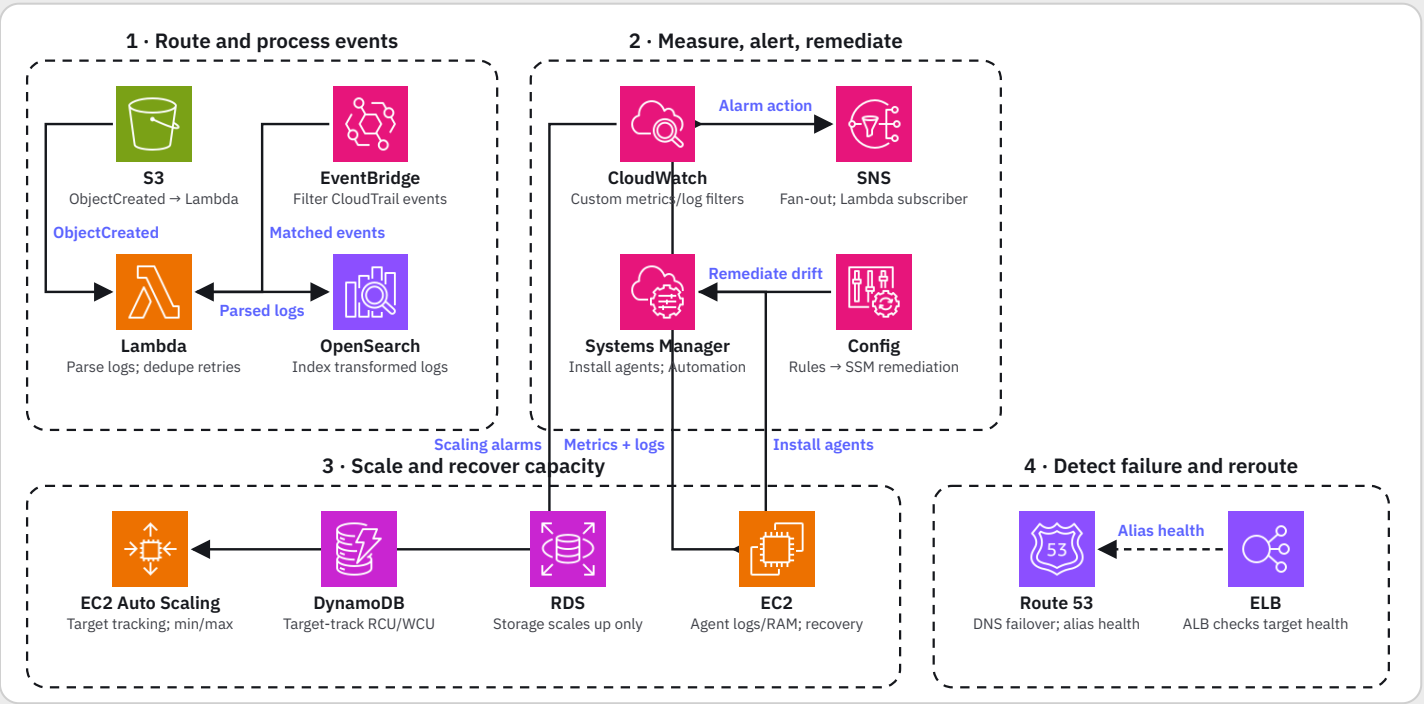
DOP-C02 · Domain 4 of 6

BlowStack

DOMAIN 4 · MONITORING AND LOGGING · TASK STATEMENT 4.3

Automate monitoring and event management of complex environments

Route, observe, scale, fail over



1 Route and process events

Use **event patterns** to match CloudTrail API events in EventBridge. S3 events trigger Lambda to parse logs into OpenSearch or CloudWatch Logs; SNS fans out, SQS buffers, and consumers must be idempotent.

2 Measure, alert, remediate

Use **CloudWatch agent** for guest memory/logs; SSM Agent enables managed actions, not metric collection. Custom metrics and log metric filters feed alarms; alarms invoke SNS, Lambda, or supported EC2 recovery actions.

3 Scale and recover capacity

Use **target tracking** for ASG/DynamoDB provisioned capacity. ECS task scaling differs from capacity-provider node scaling; EKS HPA scales pods, node autoscalers add nodes. RDS storage grows to its configured maximum.

4 Detect failure and reroute

Use **Evaluate target health** for Route 53 alias failover to an ALB; ALB health checks select targets. EC2 Auto Scaling replaces ELB-unhealthy instances only when ELB health checks are enabled.

Exam traps

- **At-least-once delivery** permits duplicate events; retries do not guarantee exactly-once processing. Deduplicate side effects, and avoid S3 processing loops with separate buckets or prefix filters.
- **EC2 recovery** handles system-status failures on supported instances; it is not an Auto Scaling replacement or a remedy for every instance-status failure.
- **Storage autoscaling** in RDS neither scales CPU nor shrinks storage. DynamoDB target tracking scales provisioned RCU/WCU; on-demand capacity needs no target-tracking policy.

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

AWS Certified DevOps Engineer - Professional Cheat Sheet

DOP-C02 · Domain 4 of 6

BlowStack

DOMAIN 4 · MONITORING AND LOGGING · WHAT TO REMEMBER

Concepts and services of Monitoring and Logging

Concepts to know

Metric Cardinality

Each unique namespace, metric name, and dimension combination identifies a metric. **Avoid unbounded dimensions** such as request IDs; they multiply time series and cost. Custom metrics do not automatically aggregate across dimensions.

Audit Logging

Audit logs record who performed which action, when, and against which resource. **Distinguish API activity from application telemetry**: CloudTrail records account activity; CloudWatch collects operational logs and metrics. Data events require explicit selection.

Event-Driven Architecture

Producers emit events that consumers process independently. **Match events, not metric thresholds**, with EventBridge rules; use CloudWatch alarms for metric conditions. Retried deliveries require idempotent remediation to prevent duplicate side effects.

Core services



Amazon CloudWatch

Use the agent for memory and disk metrics, **metric filters for log-derived metrics**, subscriptions for log forwarding, and metric streams through Amazon Data Firehose for continuous metric export.



AWS CloudTrail

Use **trails for ongoing audit delivery** to Amazon S3; event history provides 90 days of regional management events. Select data events explicitly to audit supported resource-level operations.



Amazon EventBridge

Use **event-pattern rules** to route service events, CloudTrail API events, or alarm state changes to targets. Configure target retries and a dead-letter queue for failed deliveries.

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