



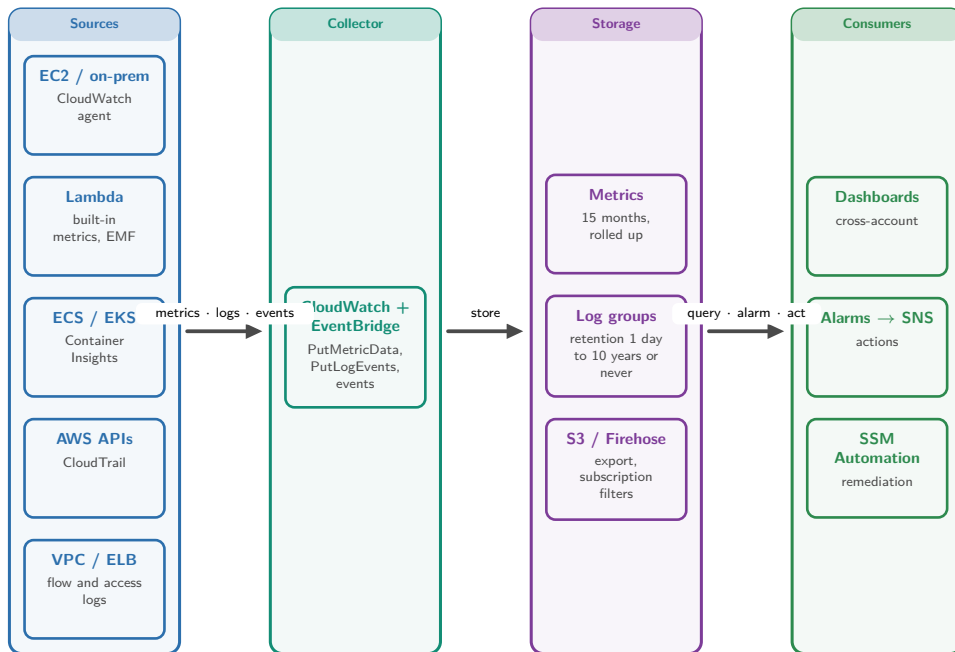
SOA-C03 Domain 1: Monitoring, Logging, Remediation

AWS Certified CloudOps Engineer Associate exam guide, as of 2026 | CloudWatch metrics, alarms, agent, Logs and Logs Insights, CloudTrail, EventBridge, Systems Manager Automation, Config remediation, Health

SOA-C03 Domain 1 CloudWatch EventBridge Systems Manager

What the domain tests

Domain 1 of SOA-C03 (about 22 % of the scored content, as of 2026, check the official exam guide) asks you to **collect** metrics and logs, **alarm** on them, **analyse** them, **remediate automatically** and **tune performance** (the performance half is on sheet 02). The successor of SysOps Administrator SOA-C02 keeps CloudWatch at the centre and adds containers (ECS, EKS), multi-account observability and more automation.



Where every signal goes in AWS: collect, store, act

Signal	Default	What you must add	Exam trap
EC2 CPU, network, disk ops	5-minute basic monitoring, free	detailed monitoring = 1-minute (paid)	memory and disk-space % are NOT default: install the CloudWatch agent
EC2 status checks	system + instance + attached EBS, 1 min	alarm with recover / reboot action	system check failed → recover (moves host), instance check → reboot

Lambda	Invocations, Errors, Duration, Throttles, ConcurrentExecutions	custom metrics via EMF	logs go to /aws/lambda/<name> only if the role can write logs
RDS	CPU, FreeStorageSpace, connections, IOPS	Enhanced Monitoring (OS, 1-60 s), Performance Insights / Database Insights	OS process list = Enhanced Monitoring, not CloudWatch metrics
ELB	RequestCount, latency, HTTP-Code_ELB_5XX, Healthy-HostCount	access logs to S3 (off by default)	5XX from ELB vs from targets: HTTPCode_Target_5XX_Count
API calls	CloudTrail event history 90 days, management events	trail for S3 storage, data events, Lake	data events (S3 object, Lambda invoke) cost extra and are off by default

Metrics and alarms

Period, evaluation periods, datapoints to alarm — An alarm with period 60 s, 5 evaluation periods and 3 datapoints to alarm fires when 3 of the last 5 one-minute points breach (M out of N).

Missing data treatment — missing, notBreaching, breaching or ignore: how gaps count; a stopped instance with breaching raises false alarms.

Metric math — Expressions over metrics such as $100 * (m1/m2)$ for an error rate, ANOMALY_DETECTION_BAND(m1, 2), FILL(m1, 0), SEARCH() across many dimensions.

Anomaly detection alarm — Alarm on a band learnt from up to two weeks of history instead of a static threshold; good for seasonal traffic.

Alarm on an error rate with M out of N

PROBLEM

Alert when the ALB 5XX error rate stays above 2 % on 3 of the last 5 minutes.

GIVEN

- m1 = HTTPCode_Target_5XX_Count (Sum, 60 s)
- m2 = RequestCount (Sum, 60 s)
- Last five minutes: 5XX = 10, 30, 25, 4, 40; requests = 1000, 1000, 1000, 1000, 1000

1

Build the expression

e1 = 100 * m1 / m2

Why: alarm on a rate, not a raw count, so traffic growth does not page you

2

Compute each point

1.0 %, 3.0 %, 2.5 %, 0.4 %, 4.0 %

Why: one point per period

3

Count breaches > 2 %

3.0, 2.5, 4.0 -> 3 of 5

Why: datapoints to alarm = 3

4

Missing-data rule

TreatMissingData = notBreaching

Why: no requests at night must not alarm

ANSWER

ALARM: 3 breaching datapoints out of 5 meet the 3/5 rule, SNS notifies the on-call topic.

CHECK

✔

With 2 of 5 breaching the alarm would stay OK; with period 300 s and 1/1 the 0.4 % point alone decides.

```
Create the alarm with the CLI (single metric version)
aws cloudwatch put-metric-alarm \
--alarm-name web-cpu-high \
--namespace AWS/EC2 --metric-name CPUUtilization \
--dimensions Name=AutoScalingGroupName,Value=web-asg \
--statistic Average --period 60 \
--evaluation-periods 5 --datapoints-to-alarm 3 \
--threshold 80 --comparison-operator GreaterThanThreshold \
--treat-missing-data notBreaching \
--alarm-actions arn:aws:sns:eu-west-3:111122223333:oncall
```

Logs, queries and the agent

A Logs Insights query built step by step

0

`fields @timestamp, @message`

1

`fields @timestamp, @message | filter @message like /ERROR/`
keep error lines only

2

`fields @timestamp, @message | filter @message like /ERROR/ | parse @message 'user=*' as user`
extract a field with a glob pattern

3

`fields @timestamp, @message | filter @message like /ERROR/ | parse @message 'user=*' as user | state count(*) as errors by user, bin(5m)`
aggregate per user per 5 minutes

4

`fields @timestamp, @message | filter @message like /ERROR/ | parse @message 'user=*' as user | stats count(*) as errors by user, bin(5m) | sort errors desc`
worst first

5

`fields @timestamp, @message | filter @message like /ERROR/ | parse @message 'user=*' as user | stats count(*) as errors by user, bin(5m) | sort errors desc | limit 20`
top 20 rows

RUN IT ON THE LOG GROUP, TIME RANGE LAST 1 H

`fields @timestamp, @message | filter @message like /ERROR/ | parse @message 'user=*' as user | stats count(*) as errors by user, bin(5m) | sort errors desc | limit 20`

Feature	What it does	Remember
Retention	per log group, 1 day to 10 years, default never expire	set retention or pay storage forever (put-retention-policy)
Metric filter	log pattern → custom metric	only new events after creation; no backfill
Subscription filter	real-time stream to Lambda, Kinesis Data Streams, Firehose, OpenSearch	up to 2 per log group; cross-account via a destination
Export to S3	create-export-task, batch, up to 12 h delay	not real time: use subscription + Firehose for streaming
Log classes	Standard vs Infrequent Access (cheaper ingestion, fewer features)	IA has no metric filters or live tail (as of 2026, check)
Live Tail	streams new events of selected log groups interactively	debugging, billed per session minute
Data protection policy	masks PII patterns (emails, keys) in log events	audit findings to another log group or S3
Cross-account observability	a monitoring account sees metrics, logs, traces of source accounts (OAM sinks and links)	replaces sharing dashboards one by one

amazon-cloudwatch-agent.json (stored in SSM Parameter Store)

```
1 {
2   "agent": {"metrics_collection_interval": 60},
3   "metrics": {
4     "append_dimensions": {"InstanceId":
5       "${aws:InstanceId}"},
6     "metrics_collected": {
7       "mem": {"measurement": ["mem_used_percent"]},
8       "disk": {"measurement": ["used_percent"],
9         "resources": ["/"]}}
10    },
11   "logs": {"logs_collected": {"files":
12     {"collect_list": [
13       {"file_path": "/var/log/nginx/error.log",
14        "log_group_name": "/web/nginx/error",
15        "retention_in_days": 30}]}}}
16 }
```

1 60 s; set 1-10 s for high-resolution metrics (more cost)

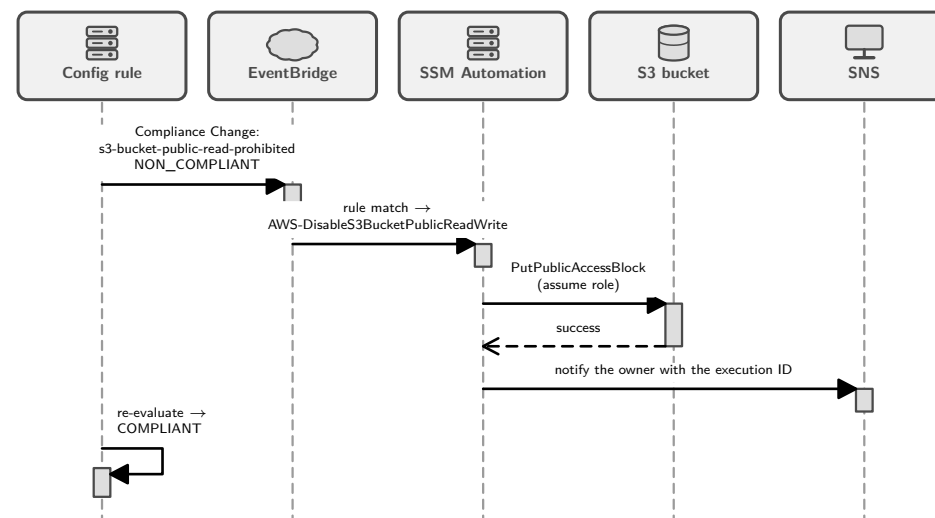
2 adds InstanceId so each server is its own series

3 memory and disk % are only available through the agent

4 ships a file to a log group; role needs CloudWatchAgentServerPolicy

Command	Use
<code>aws ssm send-command --document-name AWS-ConfigureAWSPackage --parameters name=AmazonCloudWatchAgent,action=Install</code>	install the agent on a fleet through Run Command
<code>amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c ssm:AmazonCloudWatch-web -s</code>	load the JSON config from Parameter Store and start
<code>aws logs put-retention-policy --log-group-name /web/app --retention-in-days 30</code>	stop paying for logs forever
<code>aws logs start-query --log-group-name /web/app --start-time ... --query-string '...'</code>	run Logs Insights from scripts; get-query-results to fetch

⚡ Events and automatic remediation



Detect → route → fix → notify; the same path works from a CloudWatch alarm or Security Hub finding

EventBridge pattern: EC2 instance stopped unexpectedly

```
{
  "source": ["aws.ec2"],
  "detail-type": ["EC2 Instance State-change Notification"],
  "detail": {"state": ["stopped", "terminated"]}
}
```

Tool	Fix it with	Typical exam use
CloudWatch alarm action	EC2 stop / terminate / reboot / recover, Auto Scaling policy, SNS, SSM OpsItem or incident	status check failed → recover instance
EventBridge rule	Lambda, SSM Automation, Step Functions, SNS, SQS, another bus	react to API calls (via CloudTrail), Health or GuardDuty events
Config remediation	SSM Automation document, manual or automatic with retries	re-enable encryption, remove 0.0.0.0/0 on port 22
Systems Manager Ops-Center	OpsItems aggregating alarms and events with runbooks	operational ticket queue inside AWS
Incident Manager	response plans, on-call, escalation, chat channels	page engineers for a P1 alarm (check 2026 availability: AWS announced feature changes)
AWS Health + Event-Bridge	aws.health events → Lambda or SNS	scheduled EC2 retirement → stop/start to move host

EC2 memory metric missing in CloudWatch

MEDIUM

COMMON

LIKELY CAUSES - CloudWatch agent not installed or not started - Instance role lacks CloudWatchAgentServerPolicy - No route to the CloudWatch endpoint from a private subnet	HOW TO CONFIRM Check the agent status on the host <pre>amazon-cloudwatch-agent-ctl -a status</pre>	FIX - Install and start the agent via Run Command - Attach the managed policy to the role - Add a NAT gateway or monitoring and logs interface endpoints
--	--	---

Alarm stuck in INSUFFICIENT_DATA

LOW

OCCASIONAL

LIKELY CAUSES - Wrong dimension (instance ID vs ASG name) - Metric published less often than the period	HOW TO CONFIRM List the metric with its exact dimensions <pre>aws cloudwatch list-metrics --namespace CWAgent</pre>	FIX - Copy dimensions exactly - Raise the period or set missing data to notBreaching
---	---	--

Recap and self-test

MYTH	FACT
CloudWatch shows EC2 memory by default	Memory and disk usage need the CloudWatch agent The hypervisor sees CPU, network and disk I/O, not the guest OS memory.
CloudTrail event history keeps everything	It keeps 90 days of management events Create a trail to S3 (or CloudTrail Lake) for longer retention and data events.
Exporting logs to S3 is real time	Export tasks are batch and can lag up to 12 hours Use a subscription filter to Firehose for near real-time delivery.
A metric filter counts past log events	It counts only events ingested after it is created Backfill by running a Logs Insights query instead.

Key takeaways

01

Agent for OS metrics and log files
 config in Parameter Store, role with CloudWatchAgentServerPolicy

02

Alarm on rates with M of N
 metric math, missing-data rule, composite alarms against noise

03

Logs: set retention, stream with subscriptions
 Insights for ad hoc queries, metric filters for alarms

04

Events drive remediation
 EventBridge or Config → SSM Automation runbook with an IAM role

05

Know the defaults
 5-minute EC2 metrics, 90-day event history, logs never expire

Q1

An instance fails its system status check. Which alarm action fixes it without a new instance ID?
A EC2 recover: same instance ID, private IP and EBS volumes on new hardware (instance-store data is lost).

Q2

How do you get disk-space percentage for 200 Linux instances?
A Install the CloudWatch agent with Run Command, config in Parameter Store, disk used_percent.

Q3

Which Logs feature streams events to OpenSearch in near real time?
A A subscription filter (directly, or through Firehose).

Q4

Count 'AccessDenied' lines and alarm above 10 per minute?
A Metric filter on the log group → custom metric → CloudWatch alarm (threshold 10, period 60 s).

Q5

Which service routes an S3 bucket made public to an automatic fix?
A AWS Config rule with automatic remediation (SSM Automation), or EventBridge on the compliance change.

Q6

Where do you see a scheduled EC2 retirement affecting your account?
A AWS Health Dashboard (account events), also as aws.health events in EventBridge.

Q7

Which alarm type cuts noise by combining several alarms?
A A composite alarm with AND/OR/NOT rules; children keep no actions.

Q8 How long are standard-resolution CloudWatch metrics kept?

A 15 months, rolled up: 1-minute points 15 days, 5-minute 63 days, 1-hour 455 days.

Q9 Which RDS feature shows the OS process list?

A Enhanced Monitoring (agent on the DB host, 1-60 s granularity).