AWS Certified CloudOps Engineer - Associate Cheat Sheet

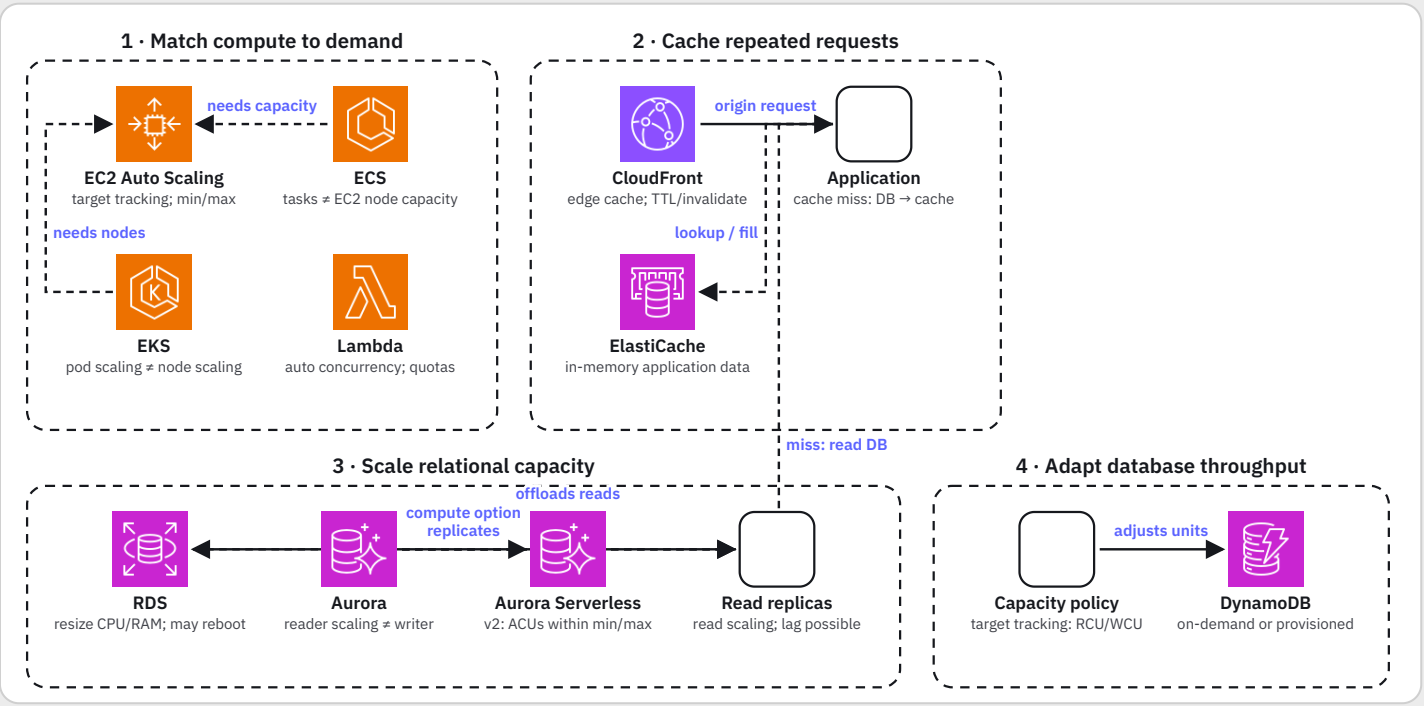
SOA-C03 · Domain 2 of 5

BlowStack

DOMAIN 2 · RELIABILITY AND BUSINESS CONTINUITY · 22% OF THE EXAM · TASK STATEMENT 2.1

Implement scalability and elasticity

Scale, cache, replicate, adapt



1 Match compute to demand

Choose **horizontal scaling** to add workers; elasticity also removes them as demand falls. ECS on EC2 needs task and capacity scaling; EKS needs pod and node scaling. Lambda scales execution concurrency automatically.

2 Cache repeated requests

Choose **cache-aside** for repeated database reads: the application checks the cache, reads the database on a miss, then fills the cache. CloudFront caches eligible origin responses; TTLs and invalidation control freshness.

3 Scale relational capacity

Choose **read replicas** for horizontal read scaling; applications must route reads to them. RDS instance resizing is vertical and can interrupt service. Aurora Serverless v2 automatically scales compute within configured bounds.

4 Adapt database throughput

Choose **on-demand** for unpredictable traffic without managing capacity units. Provisioned Auto Scaling adjusts RCU/WCU toward target utilization within bounds, with reaction delay. Hot partitions can still cause throttling.

Exam traps

- **Multi-AZ DB instance standby** provides failover, not read scaling. Read replicas serve reads; Multi-AZ DB clusters differ because their reader instances can serve reads.
- **Cache-aside does not invalidate itself** when database records change. Application updates must invalidate or refresh cached entries, or tolerate staleness until TTL expiry.
- **Reserved concurrency** reserves and caps Lambda concurrency; it does not preinitialize environments. Provisioned concurrency preinitializes environments to reduce cold-start latency.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate

AWS Certified CloudOps Engineer - Associate Cheat Sheet

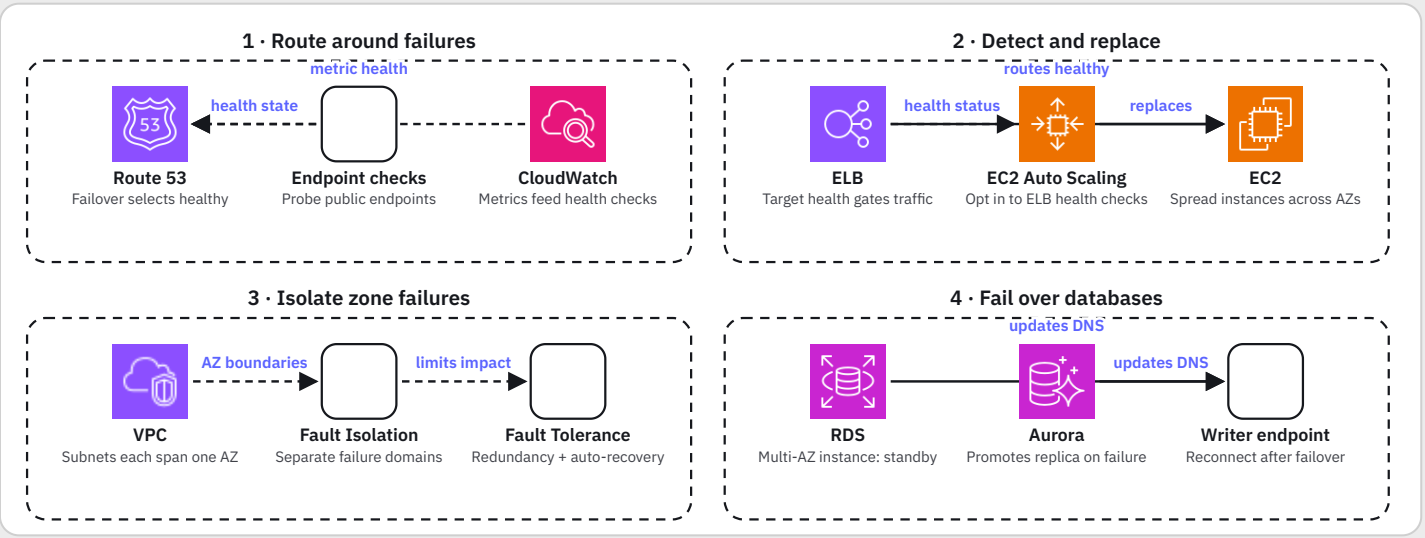
SOA-C03 · Domain 2 of 5

BlowStack

DOMAIN 2 · RELIABILITY AND BUSINESS CONTINUITY · TASK STATEMENT 2.2

Implement highly available and resilient environments

Detect, replace, isolate, fail over



1 Route around failures

DNS failover selects a healthy secondary; cached DNS delays switchover. Private endpoints need metric/alarm-based health checks rather than public endpoint probes.

2 Detect and replace

ELB health checks must be enabled on the Auto Scaling group to replace ELB-unhealthy instances. A health check grace period allows startup; load balancing alone does not replace instances.

3 Isolate zone failures

Multi-AZ needs healthy capacity and dependencies in surviving AZs. Separate subnets in one AZ do not protect against an AZ outage; redundancy needs automated recovery.

4 Fail over databases

Automatic failover switches an RDS Multi-AZ instance to its standby or promotes an Aurora replica. Place Aurora replicas across AZs; applications must reconnect using the endpoint.

Exam traps

- **Read replicas** do not replace RDS Multi-AZ instance failover. A Multi-AZ DB instance standby cannot serve reads; Multi-AZ DB clusters have readable standbys.
- **Failed ELB checks** can indicate a wrong path, port, success code, or blocked security group/NACL. EC2 status checks can pass while application health checks fail.
- **All targets unhealthy** can make a load balancer fail open. Health checks alone do not guarantee that traffic stops reaching unhealthy targets.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate

AWS Certified CloudOps Engineer - Associate Cheat Sheet

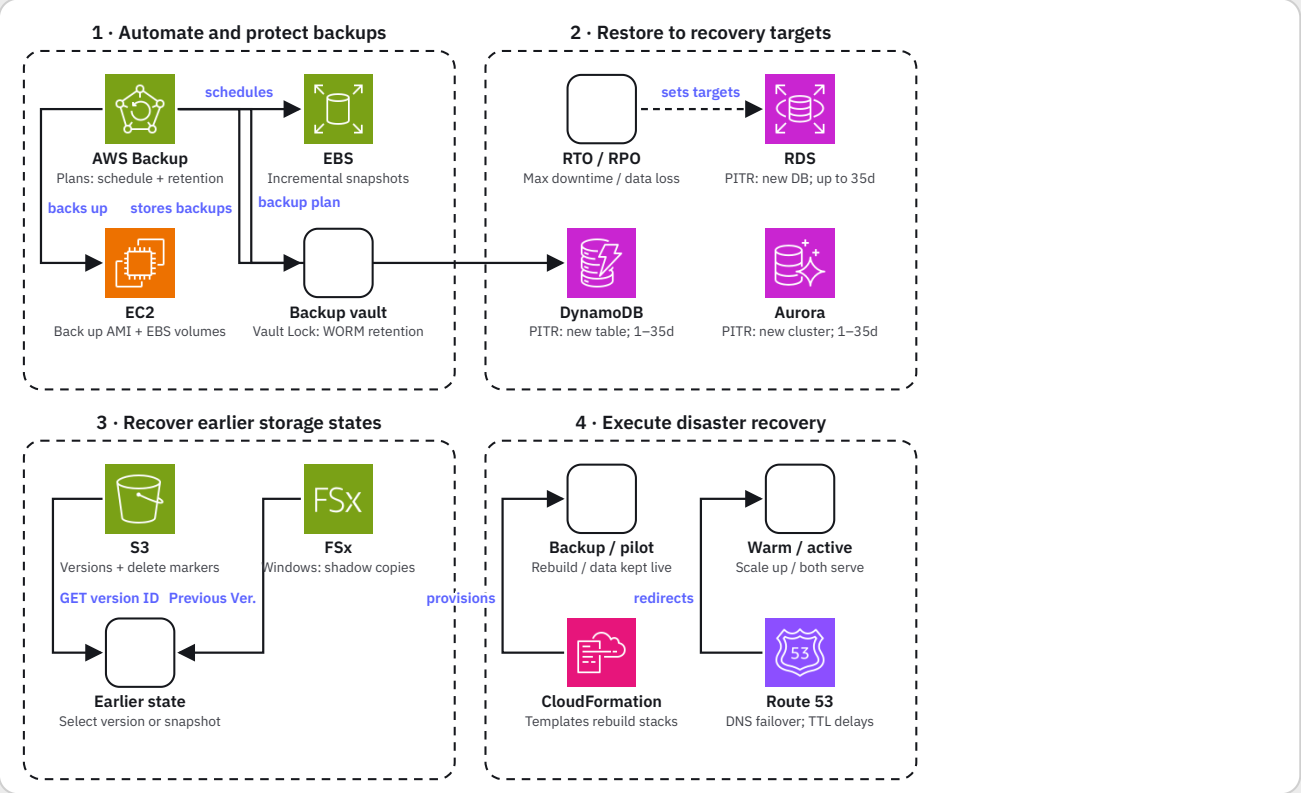
SOA-C03 · Domain 2 of 5

BlowStack

DOMAIN 2 · RELIABILITY AND BUSINESS CONTINUITY · TASK STATEMENT 2.3

Implement backup and restore strategies

Back up, restore, version, recover



1 Automate and protect backups

Use **backup plans** for scheduled protection and retention; assign resources by tags or IDs. Configure supported cross-account/Region copies explicitly. Vault Lock protects retention; restore tests verify recoverability.

2 Restore to recovery targets

Choose **PITR** for a timestamp rather than a scheduled snapshot. RDS requires automated backups; DynamoDB PITR is opt-in. Longer retention costs more. Restores create new resources; reconnect apps and validate within RTO.

3 Recover earlier storage states

Enable **versioning** on S3 to retain overwritten objects; lifecycle rules manage noncurrent-version costs. Configure FSx for Windows shadow copies for file-level recovery; file-system backups provide separate protection.

4 Execute disaster recovery

Lower RTO generally costs more: backup/restore rebuilds everything; pilot light keeps data live but starts compute; warm standby runs reduced capacity; active-active serves in both Regions. Test failover and failback.

Exam traps

- An S3 **delete marker** hides an object; it does not erase earlier versions. Deleting a specific version permanently removes that version; suspending versioning does not remove existing versions.
- An EBS snapshot is not automatically **application-consistent**. Quiesce writes or use application-aware coordination; EC2 backups do not preserve instance-store data.
- **Multi-AZ is not cross-Region DR**. Regional failures need recovery outside the Region; replication alone is not a backup because corruption or accidental changes can propagate.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate

DOMAIN 2 · RELIABILITY AND BUSINESS CONTINUITY · WHAT TO REMEMBER

Concepts and services of Reliability and Business Continuity

Concepts to know

Elasticity

Elasticity adds and removes capacity as demand changes. Choose **demand-driven scaling** for variable workloads; horizontal scaling adds resources, while vertical scaling resizes one resource and can require interruption.

Fault Tolerance

Fault tolerance keeps component failures from becoming service failures. Choose **redundancy across Availability Zones** for zonal failures; health checks, failover, and sufficient surviving capacity keep the workload available.

Recovery Time Objective

RTO limits acceptable downtime; RPO limits acceptable data loss. Choose **a recovery strategy that meets both**: backup and restore, pilot light, warm standby, and active-active generally trade increasing cost for faster recovery.

Core services



Amazon EC2 Auto Scaling

Choose **target tracking** to maintain a utilization target and scheduled scaling for predictable demand. ELB health checks must be enabled for the group to replace instances that fail those checks.



Amazon RDS

Choose **Multi-AZ for availability**, read replicas for read scaling, and point-in-time restore for recovery from unwanted changes. A traditional Multi-AZ standby does not serve read traffic.



AWS Backup

Choose **backup plans** for centralized schedules and retention across supported resources; use cross-account or cross-Region copies for isolation. Restore testing verifies recoverability and timing.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate