AWS Certified Solutions Architect - Professional Cheat Sheet

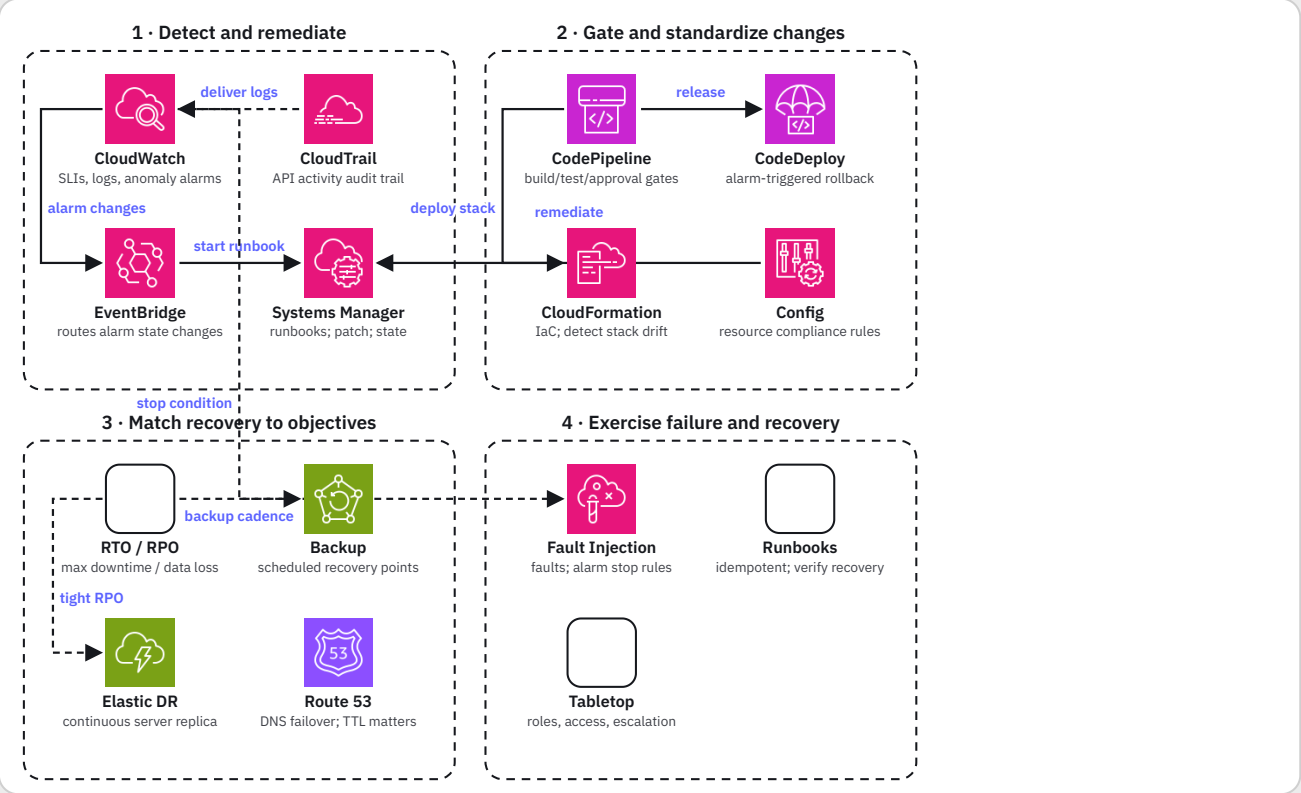
SAP-C02 · Domain 3 of 4

BlowStack

DOMAIN 3 · CONTINUOUS IMPROVEMENT FOR EXISTING SOLUTIONS · 25% OF THE EXAM · TASK STATEMENT 3.1

Determine a strategy to improve overall operational excellence

Observe, remediate, deploy, recover, rehearse



1 Detect and remediate

Alert on **user-impact SLIs**; anomaly detection suits changing baselines. Configure event rules and remediation explicitly. Structured logs and explicit retention improve investigations; automate frequent, low-risk toil first.

2 Gate and standardize changes

Choose **blue/green** for traffic-switch rollback; rolling limits simultaneous disruption but mixes versions; all-at-once risks outage. Preserve known-good artifacts and maintain data compatibility for rollback.

3 Match recovery to objectives

Choose **RTO and RPO** before architecture: backup/restore favors cost over speed; continuous server replication supports tighter objectives. Recovery still requires launch, dependency validation, traffic routing, and failback.

4 Exercise failure and recovery

Use **bounded experiments** with hypotheses, limited targets, and alarm stop conditions. Tabletop exercises test decisions; technical drills test restoration and measured RTO/RPO. Stopping fault injection does not restore every workload.

Exam traps

- **API audit is not tracing**: AWS CloudTrail records API activity; AWS X-Ray traces distributed requests. Amazon CloudWatch provides operational metrics, logs, and alarms.
- **Drift detection is not repair**: AWS CloudFormation checks supported stack properties; AWS Config evaluates resource rules. Neither automatically reverts changes without configured remediation.
- **DNS failover is not recovery**: Amazon Route 53 redirects traffic to a ready endpoint; it neither restores data nor launches servers. Backup success alone does not prove achievable RTO or RPO.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

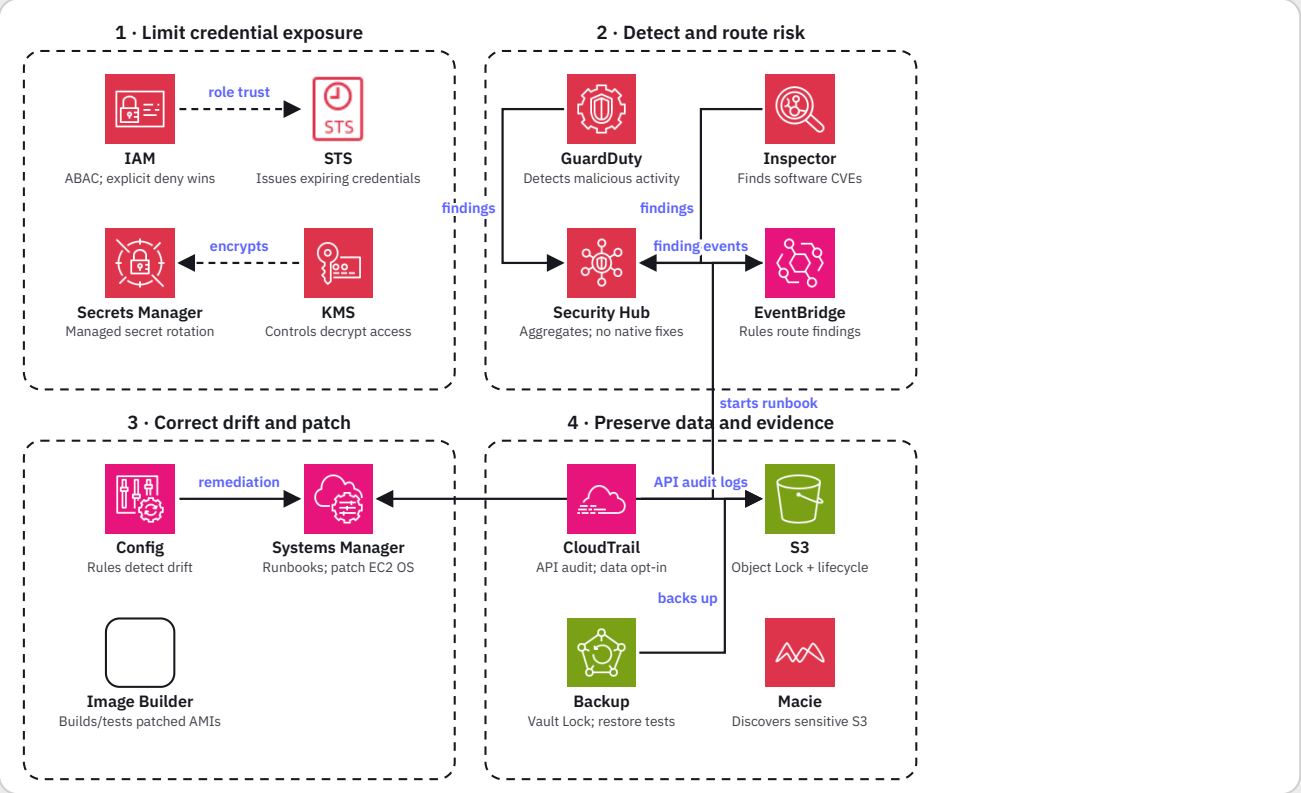
SAP-C02 · Domain 3 of 4

BlowStack

DOMAIN 3 · CONTINUOUS IMPROVEMENT FOR EXISTING SOLUTIONS · TASK STATEMENT 3.2

Determine a strategy to improve security

Authorize, detect, remediate, preserve



1 Limit credential exposure

Roles avoid distributing permanent workload keys. Secrets Manager rotation requires configuration and consumer compatibility; Systems Manager Parameter Store needs custom rotation automation.

2 Detect and route risk

Risk-based response weighs severity, exposure, and blast radius. Findings require validation; destructive containment can require approval. EventBridge routes matched events, not every finding automatically.

3 Correct drift and patch

Configured remediation needs permissions; host patching also needs managed-node connectivity. Idempotent runbooks tolerate retries. Immutable updates replace instances gradually with tested AMIs and retain rollback artifacts.

4 Preserve data and evidence

Isolated recovery separates backup administration and protects encryption keys. Residency includes replicas, backups, and logs. RPO guides backup frequency; RTO requires timed restore tests, including archive retrieval.

Exam traps

- **SCPs and permissions boundaries do not grant access**. They limit available permissions; role trust, identity policies, resource policies, and request context still affect effective access.
- **Versioning is not immutability**. S3 Object Lock protects object versions; lifecycle manages retention transitions. Backup Vault Lock compliance mode becomes unchangeable after its grace period.
- **CloudTrail log validation detects tampering; it does not prevent deletion**. Protected centralized storage preserves evidence; data events need explicit selection, and VPC traffic needs flow logs.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

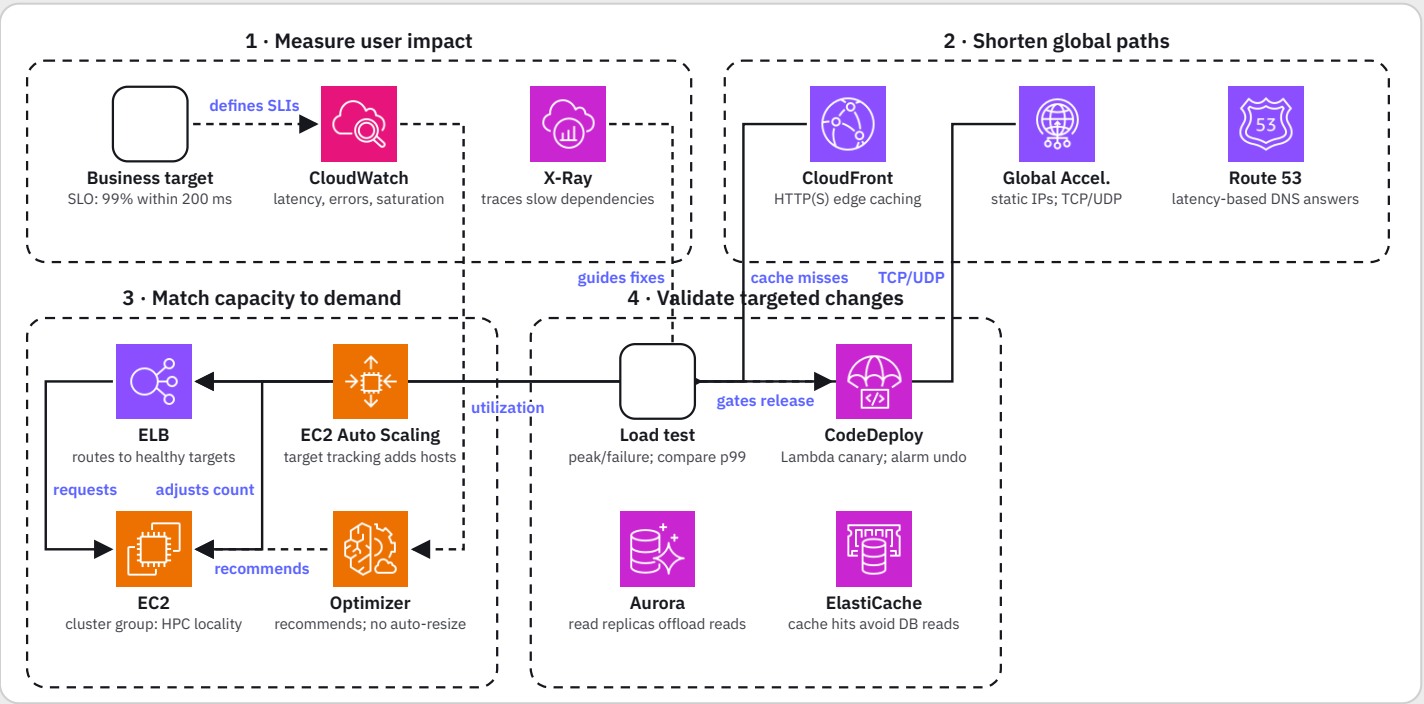
SAP-C02 · Domain 3 of 4

BlowStack

DOMAIN 3 · CONTINUOUS IMPROVEMENT FOR EXISTING SOLUTIONS · TASK STATEMENT 3.3

Determine a strategy to improve performance

Measure, accelerate, scale, validate



1 Measure user impact

Choose **user-impacting SLIs** from business KPIs; set SLOs and a measurement window. Amazon CloudWatch measures symptoms; AWS X-Ray locates slow request segments. Averages can hide tail latency.

2 Shorten global paths

Choose Amazon CloudFront for **cacheable HTTP(S)**; AWS Global Accelerator for static anycast IPs and TCP/UDP acceleration. Amazon Route 53 selects DNS answers; it does not proxy application traffic.

3 Match capacity to demand

Rightsizing matches resource shape to measured demand; horizontal scaling adds workers. Account for warm-up, quotas, and peak headroom. Parallel processing needs partitionable work; cluster placement favors low-latency HPC.

4 Validate targeted changes

Use a **representative benchmark** to compare SLO attainment and cost per successful request. Test indexes before adding database capacity; validate cache freshness. Canary traffic limits exposure; alarm-based rollback requires configuration.

Exam traps

- **SLI ≠ SLO ≠ SLA**: an SLI is the observed measurement, an SLO is its target, and an SLA is an agreement with consequences. An AWS service SLA does not guarantee application latency.
- **More instances ≠ faster requests** when database locks, missing indexes, or storage limits dominate. Amazon EC2 Auto Scaling adds capacity; Elastic Load Balancing (ELB) only distributes traffic.
- **Canary support depends on target**: AWS CodeDeploy supports canary traffic shifting for AWS Lambda and ECS, not Amazon EC2. Amazon EC2 deployments use in-place or blue/green strategies.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

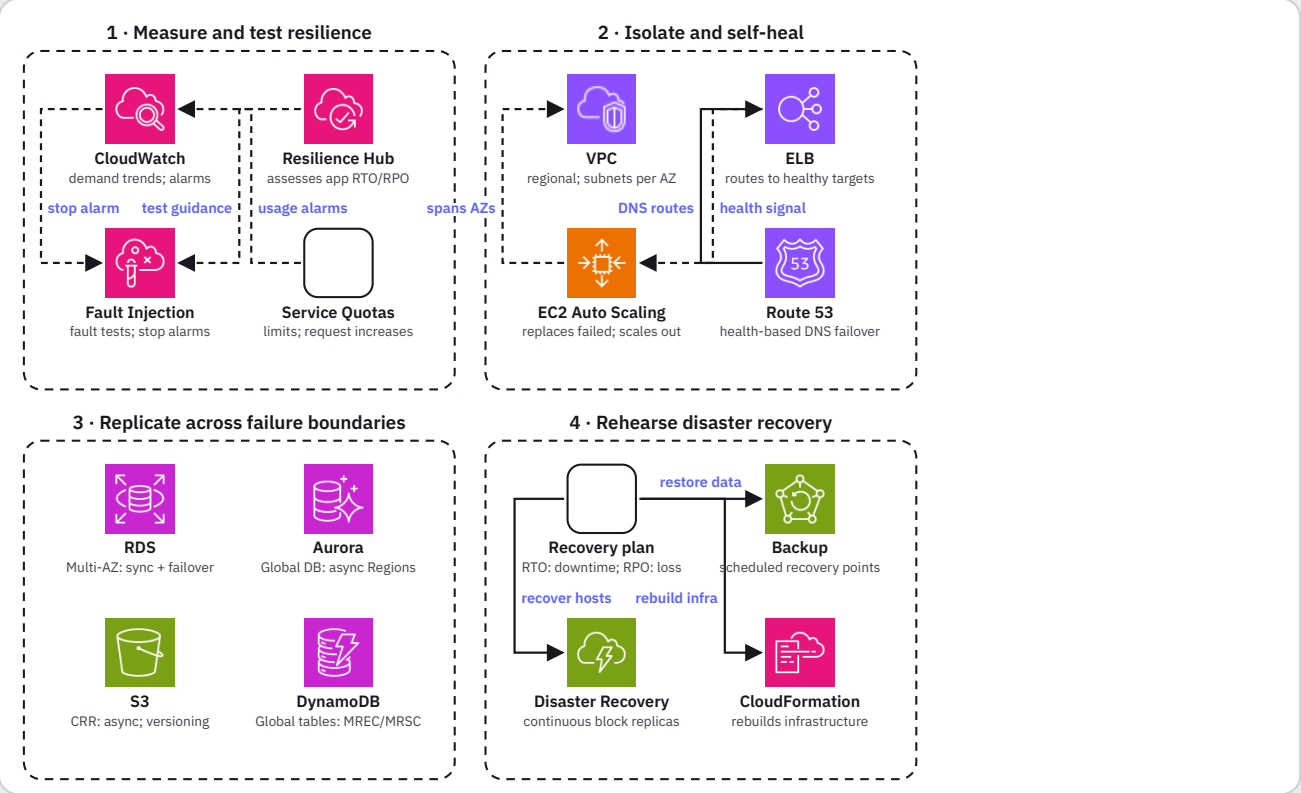
SAP-C02 · Domain 3 of 4

BlowStack

DOMAIN 3 · CONTINUOUS IMPROVEMENT FOR EXISTING SOLUTIONS · TASK STATEMENT 3.4

Determine a strategy to improve reliability

Assess, isolate, replicate, recover



1 Measure and test resilience

Use **load testing** to validate scaling and surviving-AZ headroom against demand forecasts. Architecture reviews identify risks; controlled fault experiments verify recovery under failure.

2 Isolate and self-heal

For **AZ failure**, spread capacity across AZs and enable ELB health checks in the Auto Scaling group. ELB routes; Auto Scaling replaces. DNS failover remains subject to caching and TTLs.

3 Replicate across failure boundaries

Choose **synchronous replication** for zero RPO within covered failures; asynchronous replication can lose recent writes. S3 CRR needs versioning on both buckets; existing objects need Batch Replication.

4 Rehearse disaster recovery

Choose **pilot light** for replicated core data with application capacity launched during recovery. Backup/restore costs less but takes longer; warm standby runs a scaled-down stack. Drills validate actual RTO/RPO.

Exam traps

- **RDS read replicas** usually replicate asynchronously for read scaling; promotion is not standard Multi-AZ automatic failover. A Multi-AZ DB instance standby does not serve reads.
- **Replication is not backup**: deletion or corruption can propagate. Recovery also needs usable history, infrastructure, dependencies, traffic cutover, and tested procedures.
- **Quota increases do not reserve capacity**. Request increases before growth; scaling is not instantaneous. Bound retries with exponential backoff and jitter to avoid amplifying overload.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

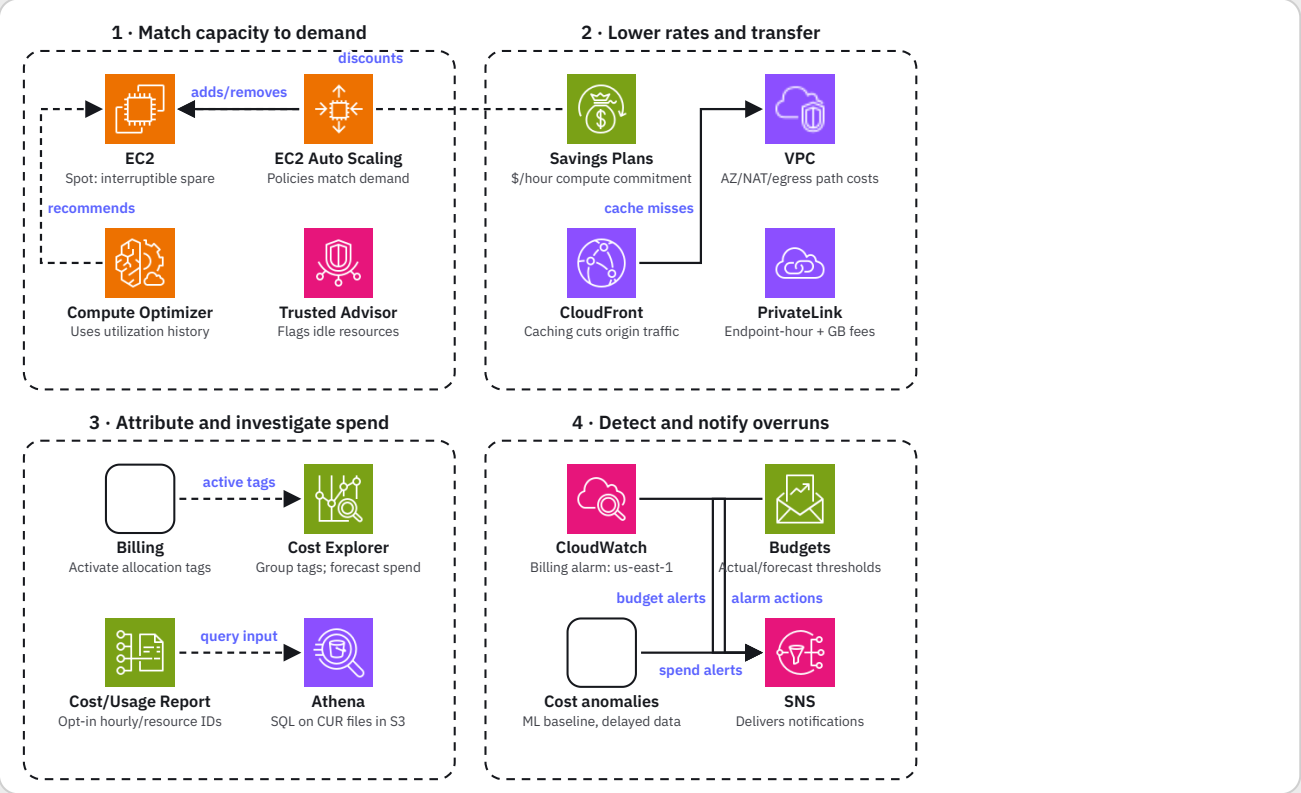
SAP-C02 · Domain 3 of 4

BlowStack

DOMAIN 3 · CONTINUOUS IMPROVEMENT FOR EXISTING SOLUTIONS · TASK STATEMENT 3.5

Identify opportunities for cost optimizations

Measure, right-size, discount, monitor



1 Match capacity to demand

Use **measured utilization** to right-size before committing; include memory and peaks. Compute Optimizer and Trusted Advisor recommend changes; Auto Scaling changes capacity through configured policies.

2 Lower rates and transfer

Commit the **predictable baseline** for 1 or 3 years; use On-Demand for uncertain demand and Spot for interruptible work. Cache repeated reads; compare data locality, NAT, endpoint and egress costs.

3 Attribute and investigate spend

Activate **cost allocation tags**, then group spend by tag/account. CUR with hourly granularity and resource IDs supports detailed Athena queries over S3 using a Glue catalog. Tag activation is not retroactive.

4 Detect and notify overruns

Use **forecast alerts** in Budgets for projected overruns, CloudWatch for fixed estimated-charge thresholds, and Cost Anomaly Detection for unusual spend. SNS distributes alerts; billing data is not real time.

Exam traps

- Savings Plans and regional RIs provide **discounts, not capacity reservations**; zonal EC2 RIs reserve capacity. Commit only to the post-rightsizing baseline.
- **Private does not mean cheaper**: PrivateLink has endpoint-hour and processing fees. Compare the actual path and volume; eliminating NAT does not eliminate every transfer charge.
- A budget is **not a hard spending cap**. Alerts do not stop resources; supported Budgets actions require configuration, and delayed billing data can allow overshoot.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

SAP-C02 · Domain 3 of 4

BlowStack

DOMAIN 3 · CONTINUOUS IMPROVEMENT FOR EXISTING SOLUTIONS · WHAT TO REMEMBER

Concepts and services of Continuous Improvement for Existing Solutions

Concepts to know

Recovery Time Objective

RTO defines **maximum acceptable downtime**. Choose a recovery strategy whose provisioning, data restoration, dependency recovery, and traffic cutover fit that limit; tighter targets generally require more standby capacity and automation.

Recovery Point Objective

RPO defines **maximum acceptable data loss measured in time**. Choose backup frequency or replication to meet it; asynchronous replication can lose recent writes, and replicas do not replace backups against corruption or deletion.

Rightsizing

Rightsizing matches resource capacity to measured demand. **Remove waste before buying commitments**; evaluate CPU, memory, throughput, latency, peak demand, and failover headroom rather than choosing smaller resources from average utilization alone.

Core services



Amazon CloudWatch

Choose **metrics and alarms** for operational health, Logs for application events, and anomaly detection for changing baselines. Alarm actions can initiate notifications or automated remediation.



AWS Systems Manager

Choose **Automation runbooks** for repeatable remediation, Patch Manager for OS patching, and State Manager for maintaining node configuration. Maintenance windows schedule controlled operational work.



AWS Config

Choose **configuration history and compliance evaluation** to detect resource-policy violations. Rules evaluate recorded configurations; remediation actions can invoke AWS Systems Manager automation.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional