AWS Certified Solutions Architect - Professional Cheat Sheet

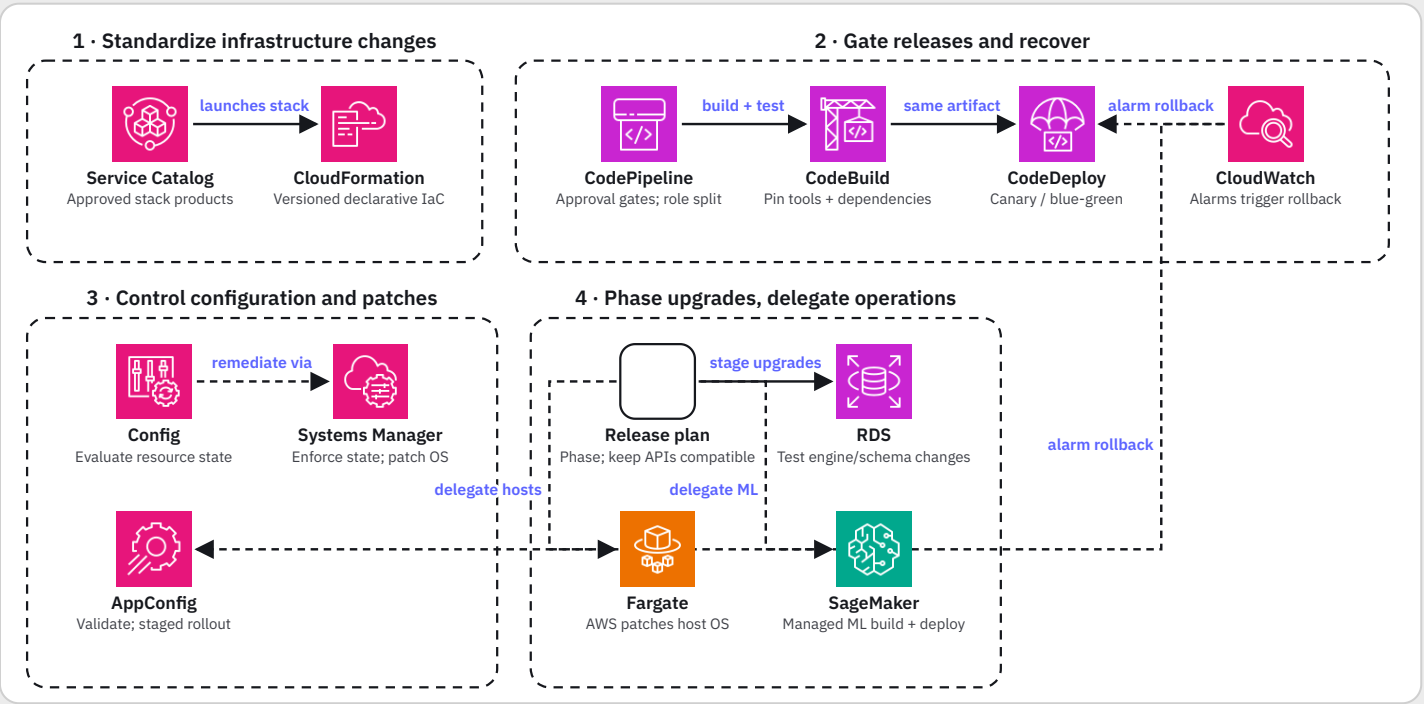
SAP-C02 · Domain 2 of 4

BlowStack

DOMAIN 2 · DESIGN FOR NEW SOLUTIONS · 29% OF THE EXAM · TASK STATEMENT 2.1

Design a deployment strategy to meet business requirements

Codify, validate, release, recover



1 Standardize infrastructure changes

Use **change sets** to review template changes before execution; AWS Service Catalog constrains self-service to approved products. Version control preserves history; review does not guarantee deployment success.

2 Gate releases and recover

Use **quality gates** for tests and independent production approval. Promote the same tested artifact; pin build inputs for reproducibility. Alarm-based rollback requires configured alarms and rollback settings.

3 Control configuration and patches

Match **configuration drift** to its layer: resource rules, OS desired state, or application settings. Remediation needs configured automation; staged configuration rollback needs health alarms.

4 Phase upgrades, delegate operations

Choose **managed services** to reduce provisioning and operational overhead, not eliminate customer duties. Phase compatible upgrades; retain application, data, and access controls. Compare total cost, not compute price.

Exam traps

- **Rollback is not data undo**: switching traffic or restoring an old artifact cannot reverse destructive schema changes. Expand, migrate, then contract only after old consumers retire.
- **Audit is not enforcement**: AWS CloudTrail records API activity; AWS Config evaluates resource state. Neither automatically patches operating systems or blocks every noncompliant change.
- **Canary support is target-specific**: AWS CodeDeploy supports canary/linear shifts for AWS Lambda and Amazon Elastic Container Service (Amazon ECS), not its EC2/on-premises deployments.

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

AWS Certified Solutions Architect - Professional Cheat Sheet

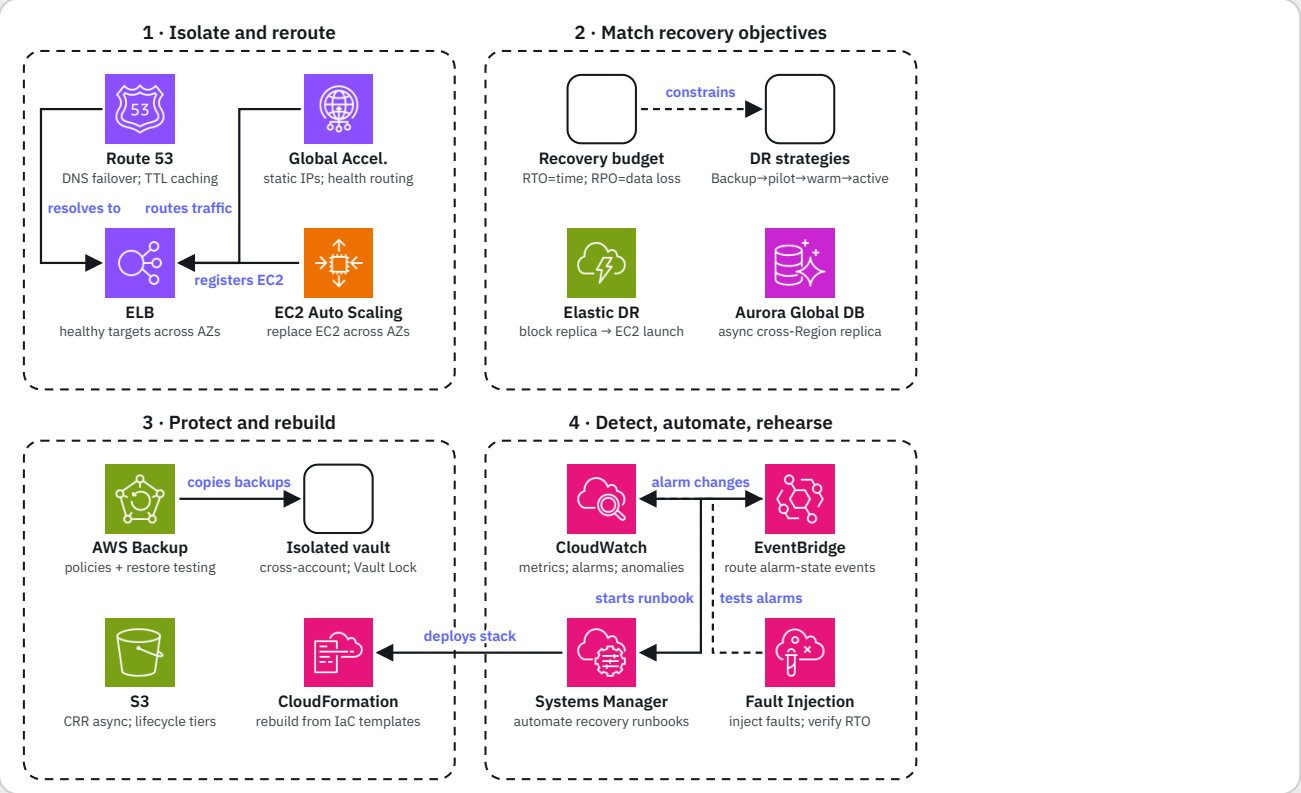
SAP-C02 · Domain 2 of 4

BlowStack

DOMAIN 2 · DESIGN FOR NEW SOLUTIONS · TASK STATEMENT 2.2

Design a solution to ensure business continuity

Isolate, replicate, restore, rehearse



1 Isolate and reroute

Multi-AZ limits the blast radius of AZ failures; multi-Region addresses regional loss. Load balancing redirects requests; scaling replaces capacity, not database state. Recovery capacity must survive the failed AZ.

2 Match recovery objectives

Pilot light keeps data/core ready but requires application capacity deployment; warm standby scales a running stack. Backup/restore is cheapest and slowest; active-active serves multiple sites but needs write-conflict handling.

3 Protect and rebuild

Isolate backups across accounts and Regions; protect retention and key access. Automate schedules, copies, and retention. Archive retrieval time counts toward RTO; infrastructure templates do not restore application data.

4 Detect, automate, rehearse

Rehearse recovery with isolated AWS Elastic Disaster Recovery drills and AWS Backup restore tests; measure actual RTO/RPO. Alarm events can start runbooks; traffic cutover, validation, and failback need orchestration.

Exam traps

- **Multi-AZ ≠ multi-Region**: Amazon RDS Multi-AZ automates in-Region failover; an ordinary read replica is not an automatic standby. Regional DR needs separate recovery resources.
- **Replication is not backup**: corruption can replicate. Amazon Aurora Global Database uses asynchronous replication; zero RPO is not guaranteed during unplanned regional failover.
- **DNS failover is not instant**: Amazon Route 53 cannot invalidate cached answers or move existing connections. AWS Global Accelerator shifts traffic behind static IPs without waiting for DNS expiry.

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

AWS Certified Solutions Architect - Professional Cheat Sheet

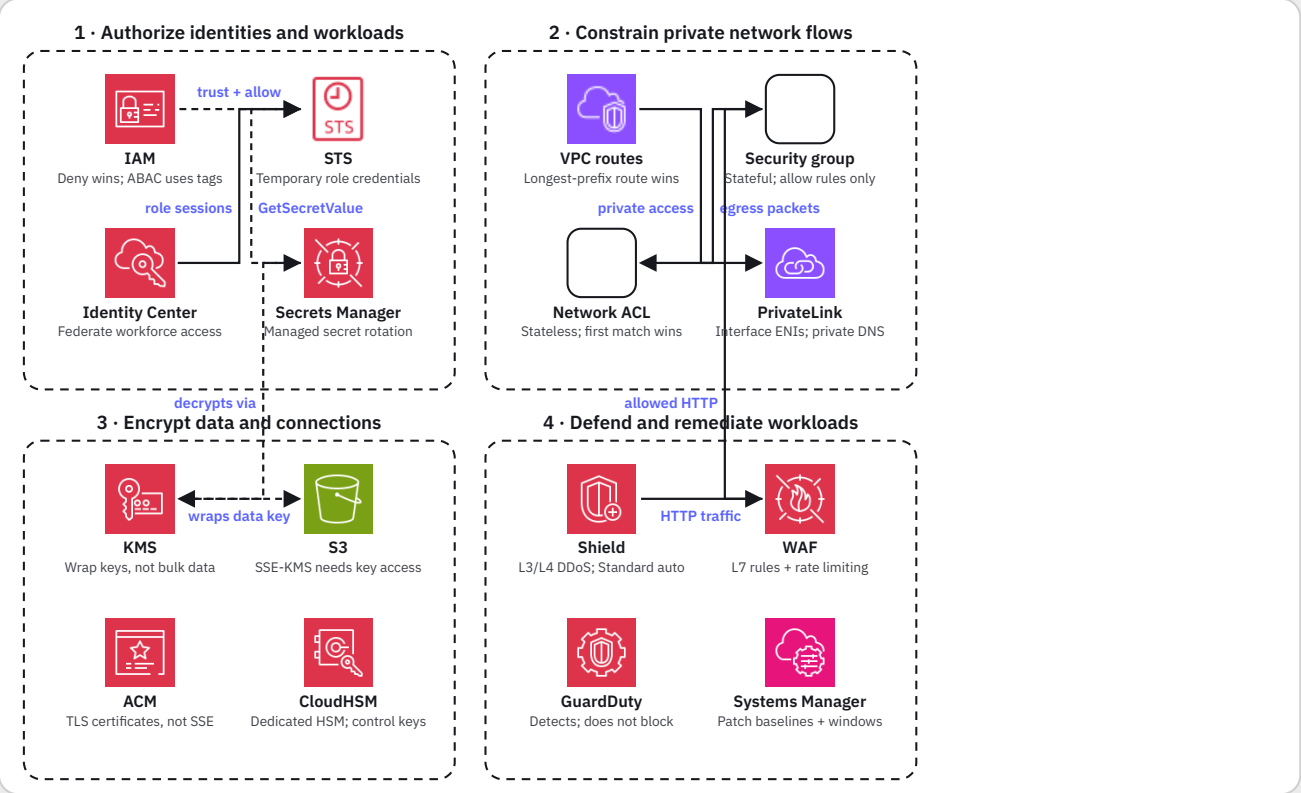
SAP-C02 · Domain 2 of 4

BlowStack

DOMAIN 2 · DESIGN FOR NEW SOLUTIONS · TASK STATEMENT 2.3

Determine security controls based on requirements

Authorize, isolate, encrypt, defend



1 Authorize identities and workloads

Roles + STS provide temporary access without stored access keys. Identity Center centralizes workforce sign-in; Secrets Manager fits secret rotation. Role trust controls who may assume; permissions control actions.

2 Constrain private network flows

Interface endpoints use PrivateLink; S3/DynamoDB gateway endpoints use route tables. SGs allow stateful returns; NACLs need both directions, including ephemeral ports. Endpoint policies restrict access, not grant it.

3 Encrypt data and connections

Envelope encryption encrypts data with a data key; KMS protects that key. TLS requirements are separate from SSE. ACM supplies certificates; CloudHSM fits dedicated, customer-controlled HSM requirements.

4 Defend and remediate workloads

Defense in depth combines Shield DDoS protection, WAF HTTP filtering, and GuardDuty detection. Systems Manager installs approved patches through configured workflows; phased rollout limits patch-failure impact.

Exam traps

- **SCPs and permissions boundaries do not grant access**; they cap permissions. Explicit deny overrides allow. Cross-account role assumption requires caller permission and target-role trust.
- **Private connectivity is not encryption**. PrivateLink avoids public network paths but does not replace TLS. S3 encryption at rest neither enforces HTTPS nor prevents authorized reads.
- **Patch compliance is not vulnerability clearance**. A baseline defines approved patches; successful installation can still leave vulnerabilities. Immutable remediation rebuilds and replaces images.

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

AWS Certified Solutions Architect - Professional Cheat Sheet

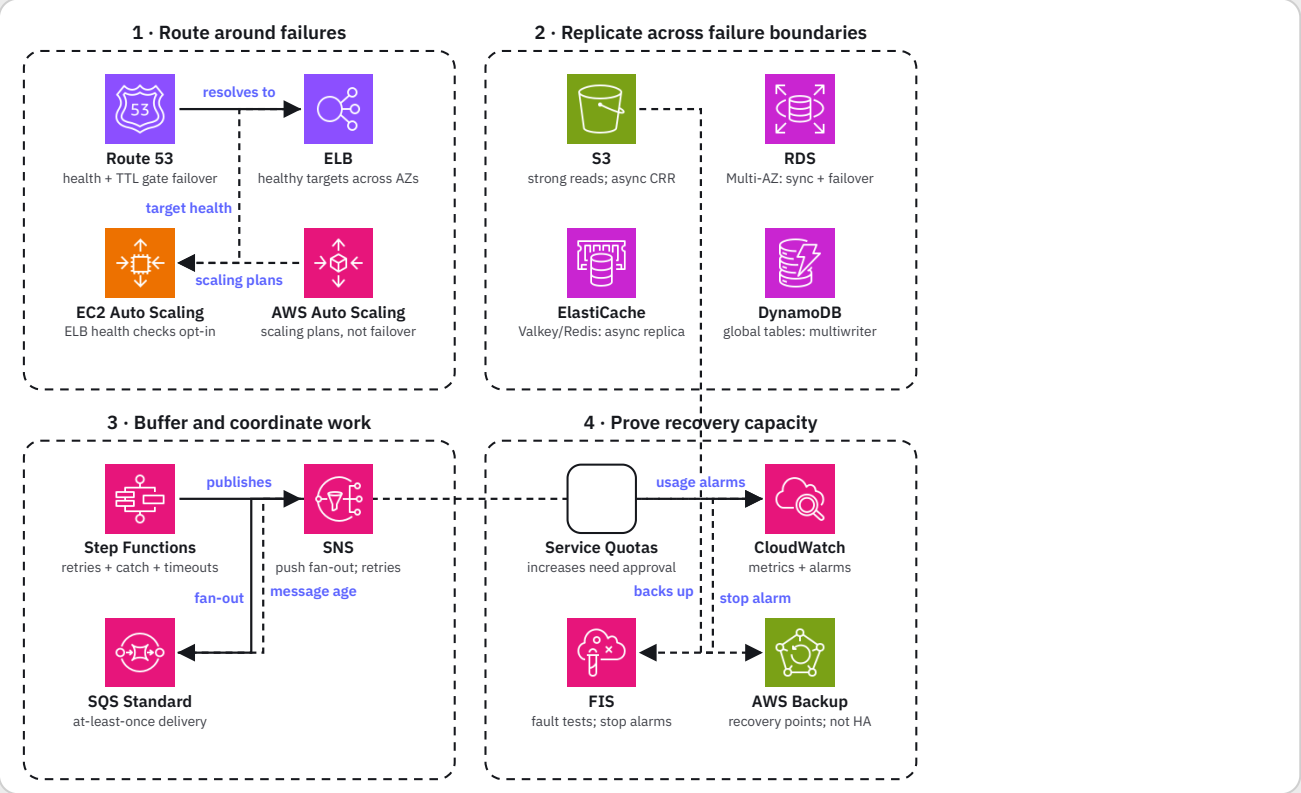
SAP-C02 · Domain 2 of 4

BlowStack

DOMAIN 2 · DESIGN FOR NEW SOLUTIONS · TASK STATEMENT 2.4

Design a strategy to meet reliability requirements

Route, replicate, decouple, recover



1 Route around failures

Use **failover routing** for active-passive; latency selects low latency, geolocation selects user location. Health checks exclude failed endpoints; DNS caches delay switching. Spread Auto Scaling capacity across AZs.

2 Replicate across failure boundaries

Regional failure needs cross-Region data, writable capacity, and routing. RDS Multi-AZ stays in one Region. Enable ElastiCache Multi-AZ automatic failover for Valkey/Redis OSS; place replicas and backups within residency rules.

3 Buffer and coordinate work

Duplicate delivery requires idempotent consumers. SQS buffers bursts; scale on backlog per worker and message age. Bound retries with exponential backoff and jitter; circuit breakers isolate failing dependencies.

4 Prove recovery capacity

RTO/RPO determine recovery design. Provision failover headroom and quota before outages; scaling is not instantaneous. Test restores and runbooks against SLOs. Fault experiments use stop alarms to bound impact.

Exam traps

- **RDS Multi-AZ DB instance** standby cannot serve reads; a Multi-AZ DB cluster has readable standbys. Read replicas are generally asynchronous; adding one does not enable automatic instance failover.
- **S3 strong consistency** does not make CRR synchronous. Durability is not availability; replication can propagate unwanted changes. Backups preserve recovery points but require restoration.
- **Composite availability** multiplies for independent mandatory serial dependencies: 99.9% × 99.9% ≈ 99.8%. Adding required dependencies can reduce end-to-end availability.

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

AWS Certified Solutions Architect - Professional Cheat Sheet

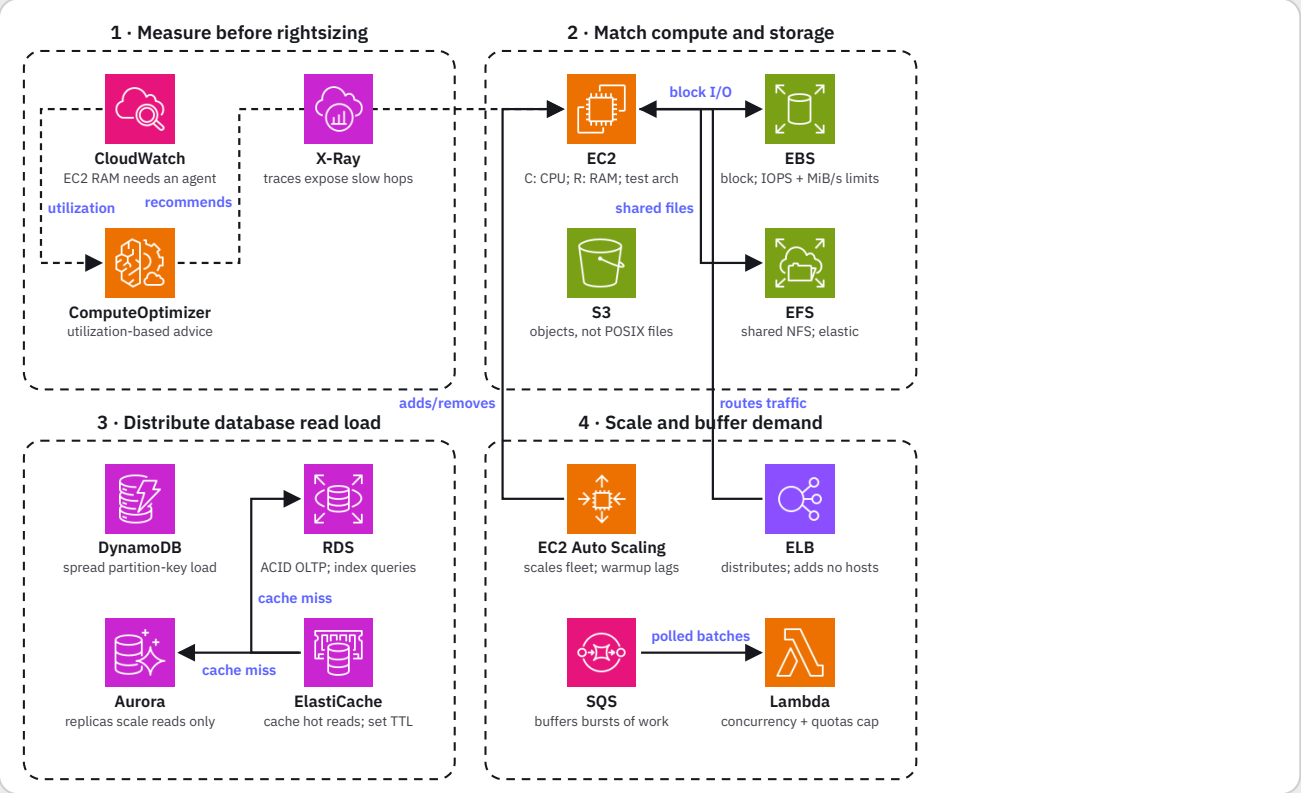
SAP-C02 · Domain 2 of 4

BlowStack

DOMAIN 2 · DESIGN FOR NEW SOLUTIONS · TASK STATEMENT 2.5

Design a solution to meet performance objectives

Measure, match, distribute, scale



1 Measure before rightsizing

Benchmark realistic load against **p99 latency SLOs**; traces locate slow dependencies, while profiling locates costly code. AWS Compute Optimizer recommends changes; it does not automatically resize resources.

2 Match compute and storage

Choose **access semantics** first: block for attached disks, objects for API access, NFS for shared files. Check x86/Arm compatibility; benchmark storage and EC2 bandwidth together, not volume IOPS alone.

3 Distribute database read load

Choose **access patterns** before engines: relational transactions favor RDS/Aurora; key-value access favors DynamoDB. Indexes add write cost. Caches need invalidation; asynchronous replicas can return stale reads.

4 Scale and buffer demand

Scale on **demand per worker**, not CPU alone; queue age and backlog reveal asynchronous demand. Schedule predictable peaks and retain warmup/quota headroom. Buffering absorbs bursts but does not shorten processing time.

Exam traps

- An RDS **Multi-AZ DB instance standby** provides failover, not read scaling. Read replicas serve reads; Multi-AZ DB clusters have readable instances.
- DynamoDB **on-demand capacity** does not eliminate hot-key throttling. Distribute partition-key traffic; extra table capacity cannot guarantee one overloaded key's performance.
- SQS-triggered Lambda processing is **at least once**, not exactly once. Idempotent handlers prevent duplicate effects; visibility timeout must accommodate processing and retries.

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

AWS Certified Solutions Architect - Professional Cheat Sheet

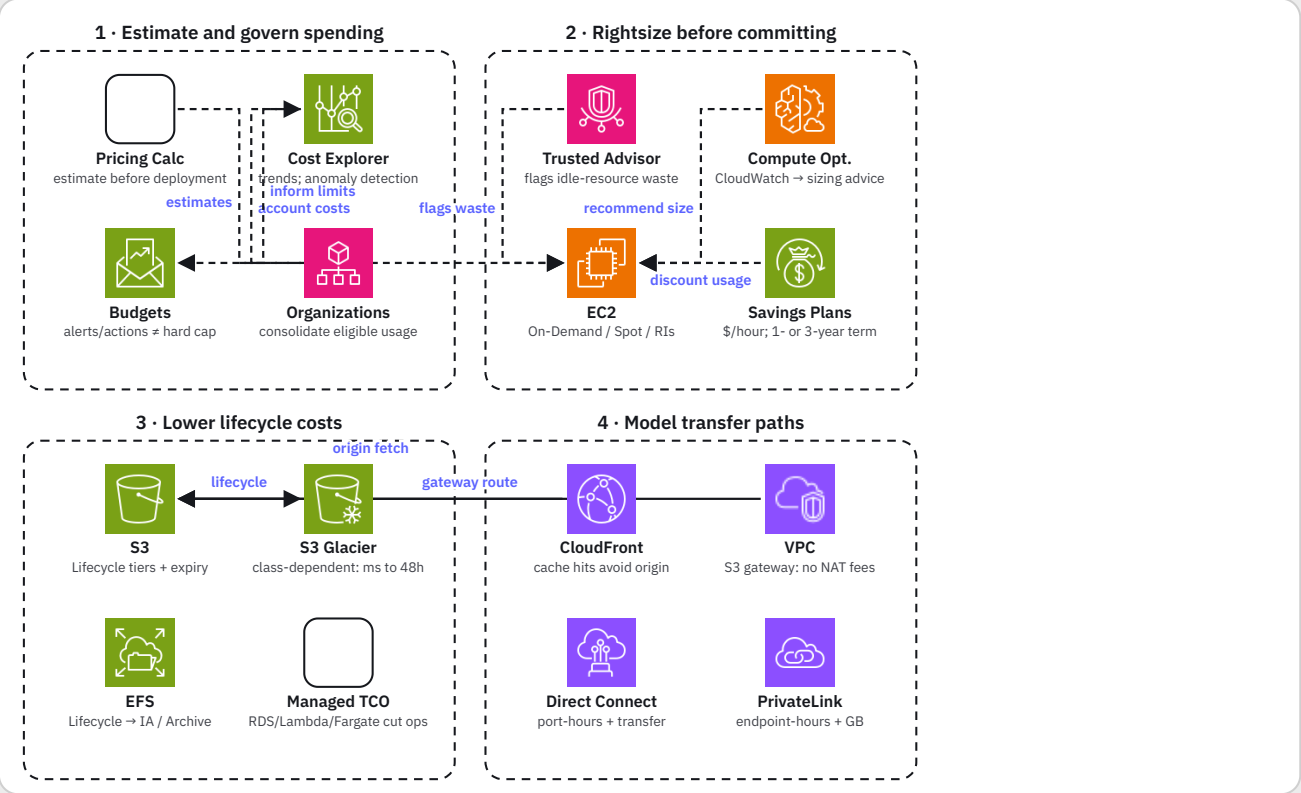
SAP-C02 · Domain 2 of 4

BlowStack

DOMAIN 2 · DESIGN FOR NEW SOLUTIONS · TASK STATEMENT 2.6

Determine a cost optimization strategy to meet solution goals and objectives

Measure, rightsize, tier, localize



1 Estimate and govern spending

Accountability: activate owner/cost-center allocation tags. Cost Explorer shows trends; AWS Cost and Usage Report gives line items. Organizations pools eligible usage for volume discounts and shares eligible discounts.

2 Rightsize before committing

Rightsize first; commit only **steady usage**. Compute Savings Plans cover EC2, Fargate and Lambda; RDS uses reserved DB instances. On-Demand fits uncertain demand; Spot fits interruption-tolerant work.

3 Lower lifecycle costs

Choose tiers by **retrieval SLA** and retention: Instant is ms; Flexible is minutes–hours; Deep Archive is hours. Include retrieval and minimum-duration charges. Managed-service TCO includes operational labor.

4 Model transfer paths

Model **bytes × path**: internet egress, cross-AZ/Region traffic, NAT and endpoint processing. Cache repeated reads; colocate chatty tiers without sacrificing availability. Direct Connect economics depend on sustained volume.

Exam traps

- AWS Budgets is **not a hard spending cap**: billing updates and actions can lag. Alerts alone do not stop resources, and budget actions require configuration.
- **Savings Plans do not reserve capacity** or discount RDS. Unused hourly commitments are still charged; commitment size follows measured usage, not interruption tolerance.
- **Private does not mean free**: PrivateLink adds endpoint and processing charges; cross-AZ paths may add transfer charges. Same Region does not imply same Availability Zone.

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

AWS Certified Solutions Architect - Professional Cheat Sheet

SAP-C02 · Domain 2 of 4

BlowStack

DOMAIN 2 · DESIGN FOR NEW SOLUTIONS · WHAT TO REMEMBER

Concepts and services of Design for New Solutions

Concepts to know

Recovery Time Objective

RTO is the maximum acceptable recovery duration. **Choose the recovery architecture**—backup and restore, pilot light, warm standby, or active-active—whose tested recovery time meets the requirement at acceptable cost.

Recovery Point Objective

RPO is the maximum acceptable data-loss window. **Choose backup frequency and replication mode** accordingly; asynchronous replication can lose recent writes, while synchronous replication protects acknowledged writes within its failure scope.

Loose Coupling

Loose coupling lets components scale and fail independently through explicit contracts. **Choose queues for buffered work**, events for routing, and orchestration for coordinated workflows; retries require idempotency and bounded backoff.

Core services

Amazon RDS

Multi-AZ provides high availability; read replicas offload reads. Cross-Region read replicas support regional recovery, but asynchronous replication introduces lag and possible data loss.

Amazon Route 53

Failover routing selects healthy endpoints; latency routing favors low-latency Regions, and geolocation routes by user location. DNS caching means traffic shifts are not instantaneous.

Amazon S3

Replication is not a historical backup. Versioning preserves earlier object versions; Object Lock protects retained versions. Lifecycle transitions trade storage savings against retrieval constraints.

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