

AWS Certified Solutions Architect – Professional (SAP-C02)

Quick Exam Refresher

*This is your condensed, high-impact review guide for the AWS Certified Solutions Architect – Professional exam. Use it just before test time to **recall key services, architectural patterns, and decision-making principles** across complex enterprise environments.*



Solutions Architect Associate (SAA-C03) Domains

This exam emphasizes building, evaluating, and evolving architectures in multi-account, multi-region, large-scale AWS environments.

- **Domain 1:** Design Solutions for Organizational Complexity – 26%
- **Domain 2:** Design for New Solutions – 29%
- **Domain 3:** Continuous Improvement for Existing Solutions – 25%
- **Domain 4:** Accelerate Workload Migration and Modernization – 20%

Quick Reminder: How the Exam Works

- **Number of Questions:** 75 total (65 scored + 10 unscored)
- **Format:** Multiple choice + multiple response
- **Time Limit:** 180 minutes
- **Passing Score:** 750/1000
- **Test Provider:** Pearson VUE (online proctored or in person)

Remember — You Don't Need to Be Perfect to Pass

The passing score is **750/1000**, so you can miss around **12–15 scored questions** and still succeed. Focus on selecting the *most appropriate* architecture based on trade-offs — not recalling trivia.

Domain 1: Design Solutions for Organizational Complexity (26%)

Multi-Account Strategy

- Use AWS Organizations to manage accounts.
- Organize with OUs (Prod, Dev, Security) and apply SCPs for guardrails.
- Centralize billing and share RIs/Savings Plans.
- Use IAM Identity Center (SSO) for unified access.
- Share resources using AWS Resource Access Manager.

Networking Across Accounts

- Use AWS Transit Gateway for scalable VPC-to-VPC connectivity.
- Prefer PrivateLink or VPC Endpoints to keep traffic inside AWS.
- Use Route 53 Resolver endpoints for hybrid DNS resolution.
- Avoid overlapping CIDRs; if you have them, use specific routing.

Security Controls

- Use IAM roles, not users, for cross-account access.
- Apply SCPs to restrict actions across accounts.
- Enable AWS Config, CloudTrail, GuardDuty, and Security Hub.
- Encrypt everything with AWS KMS. Use customer-managed keys for compliance.
- Use centralized logging account for CloudTrail and VPC Flow Logs.

Resilience & High Availability

- Design for multi-AZ (app servers, RDS, etc.).
- Use Route 53 health checks and failover routing.
- Disaster Recovery strategies: Backup & Restore, Pilot Light, Warm Standby, Active-Active.
- Understand RTO/RPO tradeoffs.

Cost Visibility & Optimization

- Use Cost Explorer, AWS Budgets, and Cost and Usage Reports.
- Tag resources for tracking.
- Purchase RIs/Savings Plans for steady usage.
- Use Spot Instances for fault-tolerant workloads.
- Share NAT Gateways, endpoints, and Direct Connect via Transit Gateway.

Domain 2: Design for New Solutions

(29%)

Infrastructure as Code & CI/CD

- Use CloudFormation or CDK to automate resource deployment.
- Use CodePipeline, CodeBuild, CodeDeploy for CI/CD.
- Implement Blue/Green, Canary, or Rolling deployments.
- Store configs/secrets in Parameter Store or Secrets Manager.

High Availability & DR

- Multi-AZ as default for all tiers.
- Use Aurora Global Database for cross-region RTO/RPO.
- Leverage S3 CRR for cross-region replication.
- Use Route 53 latency-based or failover routing for multi-region apps.

Security by Design

- Use IAM roles with least privilege.
- Encrypt data in transit and at rest.
- Design subnets (public/private), restrict SG/NACLs.
- Use AWS WAF, Shield, and AWS Firewall Manager where applicable.

Performance Efficiency

- Use Auto Scaling, ALB/NLB, ElastiCache, DynamoDB with DAX.
- Use CloudFront and Global Accelerator for global latency optimization.
- Use ENA and placement groups for HPC/low latency.

Cost Efficiency

- Use S3 lifecycle rules, DynamoDB on-demand, Aurora Serverless v2.
- Right-size EC2 with Compute Optimizer.
- Use Fargate for spiky workloads to avoid idle EC2.
- Store logs in S3/Glacier, not in active systems.

Domain 3: Continuous Improvement for Existing Solutions (25%)

Operational Excellence

- Automate patching with Systems Manager Patch Manager.
- Use Systems Manager Automation for runbooks and remediation.
- Review CloudWatch metrics and dashboards regularly.
- Use CloudTrail Insights and GuardDuty findings for alerts.

Security Posture

- Scan instances with Amazon Inspector.
- Review IAM roles/users for over-permissioning.
- Enable AWS Security Hub and Config conformance packs.
- Encrypt logs and enable log integrity validation.
- Regularly rotate access keys and secrets.

Performance Improvements

- Analyze performance bottlenecks using X-Ray, CloudWatch, RDS Insights.
- Use caching (ElastiCache), read replicas (RDS), parallel Lambda execution.
- Switch EBS gp2 to gp3 for performance and cost control.

Reliability Enhancements

- Add Multi-AZ or global failover to RDS/DynamoDB.
- Implement backups with AWS Backup (cross-region optional).
- Improve failure detection with Route 53 health checks.
- Test with AWS Fault Injection Simulator or GameDay exercises.

Cost Optimization

- Review Trusted Advisor and Cost Explorer for unused resources.
- Implement start/stop schedules for non-prod environments.
- Move infrequently accessed data to IA/Glacier.
- Identify long-running workloads for Savings Plans.

Domain 4: Accelerate Workload Migration and Modernization (20%)

Migration Planning

- Use AWS Migration Hub and Discovery tools.
- Classify applications into the 7 Rs: Rehost, Replatform, Refactor, etc.
- Use AWS Application Migration Service (MGN) for lift-and-shift.
- Use AWS DMS and SCT for database migrations.

Migration Execution

- Use AWS Snowball for large data transfers.
- Use DataSync for file-based workloads (NAS to EFS/S3/FSx).
- Test with non-disruptive launches via MGN.
- Validate cutover with health checks and rollback planning.

Post-Migration Optimization

- Transition RDS to Aurora for performance/cost.
- Move static content to S3 + CloudFront.
- Migrate monolith to microservices (Strangler Fig pattern).
- Replace queue systems with SQS/SNS, API gateways, or Step Functions.

Modernization Paths

- Use ECS/EKS/Fargate for containerized apps.
- Use Lambda + EventBridge for event-driven workflows.
- Use Aurora Serverless, DynamoDB, and managed services to reduce ops burden.
- Apply Well-Architected Framework reviews to optimize migrated systems.

Core AWS Services You Must Know

(High Priority – Frequently Tested)

Service	What You Must Know
EC2	Instance types, Auto Scaling, placement groups, savings plans, right-sizing, Spot/On-Demand/RI mix.
VPC	CIDR blocks, subnets, routing, security groups, NACLs, NAT Gateways, Internet Gateways.
IAM	Roles, policies, trust relationships, STS, cross-account access, least privilege.
S3	Storage classes, bucket policies, CRR, versioning, encryption (SSE-KMS), lifecycle rules.
RDS	Multi-AZ, read replicas, backups, failover, snapshot restore, Aurora Global Database.
Route 53	DNS routing types (latency, failover, weighted, geolocation), health checks.
ELB (ALB/NLB)	Load balancing across AZs, health checks, path-based routing, listener rules.
CloudWatch	Metrics, alarms, dashboards, custom metrics, log monitoring, anomaly detection.
CloudTrail	API logging, multi-region trail, log aggregation, integration with SIEM.
Organizations	OU structure, consolidated billing, SCPs, account isolation strategies.
KMS	Customer-managed keys, key policies, envelope encryption, cross-account access.
Lambda	Event-driven compute, timeout limits, concurrency, CI/CD deployments, use in workflows.
SQS	Decoupling components, dead-letter queues, message retention, scaling consumers.
SNS	Pub/sub messaging, cross-account topic access, fan-out architecture.

CloudFormation	StackSets, change sets, drift detection, automation of environments.
ECS / EKS	Container orchestration, Fargate use cases, task definitions, EKS node groups.
DMS	Homogeneous/heterogeneous DB migrations, CDC, downtime minimization, integration with SCT.
Application Migration Service (MGN)	Lift-and-shift of VMs, replication, cutover testing, boot config.
GuardDuty	Threat detection, VPC Flow Log analysis, AWS account compromise indicators.
Config	Resource change history, conformance packs, remediation via SSM automation.
WAF & Shield	DDoS protection, IP blocking, web ACLs, OWASP mitigation for apps.
Transit Gateway	Hub-and-spoke VPC and hybrid connectivity, route domains, scaling beyond peering.
Direct Connect	Hybrid networking, private virtual interfaces, redundancy with VPN.
SSM (Systems Manager)	Session Manager, Patch Manager, Parameter Store, maintenance windows.

Other AWS Services You Should Know

(Moderate Priority – Occasionally or Partially Tested)

Service	What You Must Know
IAM Identity Center (SSO)	Centralized identity management, federation, access assignments.
AWS Backup	Centralized backup service, cross-region, across services like EBS, RDS, DynamoDB.
Elastic Beanstalk	PaaS abstraction, environment tiers, blue/green deployments.
AWS Cost Explorer	Analyze usage trends, RI/SP coverage, filtering by tags/accounts.
AWS Budgets	Cost alerting, budget actions, thresholds by service/account.
CloudFront	Edge caching, geo restriction, origin failover, signed URLs.
Global Accelerator	TCP/UDP acceleration, static IPs, health-based routing to regions.
S3 Glacier	Archive tier, retrieval tiers, lifecycle transitions.
Athena	Serverless querying of S3, use cases in log analysis.
Step Functions	Workflow orchestration, error handling, integration with Lambda/ECS.
AppConfig	Feature flagging, deployment safety, validation strategies.
Macie	PII detection in S3, alerts, use in compliance scanning.
Inspector	Vulnerability management, EC2 scans, container image assessments.
Security Hub	Centralized security findings, CIS benchmark checks.

Trusted Advisor	Cost optimization, performance, security recommendations.
EFS	Shared file storage, throughput modes, backup integration.
FSx (Windows/Lustre)	File system performance options, domain join (FSx for Windows).
AWS Glue	ETL service, job triggers, integration with S3 and Redshift.
CodePipeline	CI/CD orchestration, stages, integration with CodeBuild/Deploy.
CodeBuild	Build environment configuration, caching, parallel builds.
CodeDeploy	Deployment strategies (canary, blue/green), rollback, ECS/Lambda targets.
EventBridge	Event bus, filtering, cross-account rules, SaaS integration.
Cognito	User pools, federation, token issuance, fine-grained IAM roles.
VPC Lattice	(New) Application-layer routing across VPCs, simplify service-to-service auth.
Workspaces	Virtual desktop environments, often seen in hybrid design questions.
AWS Control Tower	Multi-account landing zone automation, guardrails, governance setup.
ElastiCache	Redis/Memcached caching layer, performance optimization.
DynamoDB	On-demand/provisioned, DAX, TTL, global tables, PITR.
Aurora	Cluster architecture, serverless v2, read scaling, global DB.
Redshift	Data warehouse, concurrency scaling, Spectrum, integration with BI tools.

Snow Family	Data transfer at petabyte scale, use cases with limited connectivity.
DataSync	Transfer large datasets, on-prem NAS to AWS services.
Service Catalog	Controlled product deployments across teams/accounts.
App Runner	Simple web service deployment from code or container.
Timestream / QLDB	Niche database services for specific use cases.