AWS CERTIFIED
SAP-C02

Solutions Architect
Professional

QUICK REFERENCE
75 Questions · 180 Min · 750/1000 to Pass
4 Domains · No Penalty for Guessing

D1 · Organizational Complexity 26% | D2 · New Solutions Design 24% | D3 · Migration & Modernization 26% | D4 · Cost & Performance 24%

DOMAIN 1 · ORGANIZATIONAL COMPLEXITY 26%

AWS Organizations & SCPs
- SCPs = maximum permissions — they do NOT grant access on their own
- Deny in SCP overrides any Allow; management account is IMMUNE to SCPs
- OU hierarchy: SCPs cascade down to all member accounts in the OU
- Use Deny-list (default) or Allow-list strategy — allow-list is more restrictive
- Consolidated Billing: volume discounts, single payer, RI/Savings Plans sharing

AWS Control Tower
- Automates multi-account "landing zone" setup using Organizations + SSO + Config
- Preventive guardrails → SCPs (stop non-compliant actions)
- Detective guardrails → AWS Config rules (detect violations after the fact)
- Account Factory: vending machine for new accounts with baseline guardrails
- Customizations for Control Tower (CfCT): GitOps for SCP + Config + CfnStackSets

Resource Access Manager (RAM)
- Share: subnets, Transit GW, Route53 Resolver rules, License Manager configs
- Shared subnets → workloads in member accounts; central team manages routing
- Eliminates duplicated NAT GWs / VPC Endpoints across accounts

IAM Identity Center (SSO)
- Recommended for multi-account human access (replaces per-account IAM users)
- Connect to external IdP: Okta, Azure AD, Active Directory via SAML 2.0 / SCIM
- Permission Sets → mapped to OU/account combinations in Organizations
- ABAC: assign tags to users; use tag conditions in permission policies

Advanced IAM Patterns
- **Permission Boundaries**: cap max perms for roles/users; admin delegates safely
- **External ID**: confused-deputy prevention for cross-account third-party roles
- **Service Control Policy vs RCP**: SCP restricts principals; RCP restricts resources
- **Attribute-Based Access Control**: tag-driven policies scale to many resources

Hybrid Networking
- Transit Gateway: hub-and-spoke; inter-region peering; route tables per TGW
- TGW route table segregation: prod vs dev — associate + propagate selectively
- DX Gateway: connect one Direct Connect to multiple VPCs across regions/accounts
- Site-to-Site VPN over DX: IPSec encryption on private VIF for compliance
- AWS Network Firewall: managed stateful/stateless inspection in centralized VPC
- VPC Endpoint (Gateway): S3 & DynamoDB free; Interface: other services, has SG

DOMAIN 2 · NEW SOLUTIONS DESIGN 24%

Well-Architected Framework (6 Pillars)
- **Operational Excellence**: IaC, runbooks, small reversible changes, observe
- **Security**: least privilege, protect data in-transit/at-rest, trace events
- **Reliability**: auto-recover, test recovery, horizontal scale, no single points
- **Performance Efficiency**: use managed services, experiment, go global fast
- **Cost Optimization**: measure ROI, use Spot/Savings Plans, right-size
- **Sustainability**: minimize footprint, use managed services, measure impact

Decoupling & Event-Driven Patterns
- SQS: queue, at-least-once delivery, up to 14-day retention, max 256KB msg
- SNS fan-out: one publish → multiple SQS/Lambda/HTTP endpoints in parallel
- Kinesis Data Streams: ordered per shard, replay up to 7 days, 1MB/s per shard
- Kinesis vs SQS: ordered + replay → Kinesis; scale infinitely + decouple → SQS
- EventBridge: event bus, schema registry, cross-account routing, archive + replay
- Step Functions Standard: 1-year, exactly-once, full audit, up to 2,000 states/s
- Step Functions Express: 5-minute max, at-least-once, high-throughput (100k/s)

Databases & Caching
- Aurora Global DB: multi-region active-passive; <1s RPO; ~1 min RTO on promote
- DynamoDB Global Tables: multi-region active-**active**; last-writer-wins CRDTs
- ElastiCache Redis: session store, leaderboard, pub/sub, complex data structures
- DAX: in-memory DynamoDB accelerator; microsecond reads; write-through cache
- RDS Proxy: pool connections; reduce aurora/RDS cold-start for Lambda workloads

Disaster Recovery Strategies
- **Backup & Restore**: RPO/RTO hours — cheapest; restore from S3/RDS snapshots
- **Pilot Light**: minimal always-on core (DB replicated); scale up on disaster
- **Warm Standby**: scaled-down replica always running; rapid scale-out
- **Multi-Site Active-Active**: zero downtime; most expensive; Route 53 weighted

Modern Architecture Patterns
- Strangler Fig: wrap legacy; route traffic incrementally to microservices
- CQRS: separate read (Query) model from write (Command) model
- Saga Pattern: choreography (events) or orchestration (Step Functions) for txns
- CloudFront + OAC: replace OAI; use origin access control for S3 secure delivery
- Lambda Provisioned Concurrency: pre-warm; eliminates cold starts for latency SLA

DOMAIN 3 · MIGRATION & MODERNIZATION 26%

The 7 Rs of Migration

- **Retire**: decommission — 10-20% of portfolio often just turned off
- **Retain**: keep on-premises; not ready or not worth migrating yet
- **Rehost**: lift-and-shift; fastest path; use AWS MGN agent-based replication
- **Relocate**: VMware Cloud on AWS; move VMware workloads, no agent needed
- **Repurchase**: move to SaaS (Salesforce, ServiceNow, Workday)
- **Replatform**: minor optimizations — e.g., Oracle → RDS, Tomcat → Elastic Beanstalk
- **Refactor / Re-architect**: cloud-native redesign; Lambda, containers, managed DBs

Database Migration

- DMS: Homogeneous migration (same engine) → DMS only; continuous CDC support
- DMS + SCT: Heterogeneous (e.g., Oracle → Aurora) → SCT converts schema first
- SCT generates assessment report: conversion complexity per object
- DMS tasks: Full Load | Full Load + CDC | CDC Only — minimize downtime strategies
- AWS Schema Conversion Tool standalone handles stored procs, views, triggers

Server & Data Migration Tools

- AWS MGN (Application Migration Service): primary rehost tool; replaces SMS
- MGN: continuous block-level replication; minimal cutover window (~minutes)
- Application Discovery Service: agentless (VMware vCenter) or agent-based
- Migration Hub: central tracking dashboard; integrates MGN, DMS, SMS, SCT
- Elastic Disaster Recovery (DRS): same as MGN architecture; for DR use-case

Data Transfer & Hybrid Storage

- DataSync: online, incremental, scheduled — NFS/SMB/S3/EFS/FSx to AWS
- Snowball Edge Storage: 80TB usable; encrypt at-rest; good for >10TB / poor WAN
- Snowmobile: 100PB per truck — exabyte scale; physical data center transfer
- DataSync vs Snow: DataSync = online recurring | Snow = offline one-time large
- Storage Gateway: File (NFS/SMB→S3), Volume (iSCSI cached/stored), Tape (VTL)

VMware & Container Modernization

- VMware Cloud on AWS: vSphere SDDC on dedicated hosts; HCX for live migration
- ECS vs EKS: ECS = simpler AWS-native; EKS = K8s compatible, more portable
- Fargate: serverless containers; no EC2 management; supports ECS and EKS
- App2Container (A2C): containerize existing Java/.NET apps; generates ECS/EKS

DOMAIN 4 · COST & PERFORMANCE OPTIMIZATION 24%

EC2 Purchasing Options

- On-Demand: no commitment, pay per second; baseline for unpredictable workloads
- Reserved Instances (1 or 3yr): up to 72% off; Standard (sell on MP) or Convertible
- Savings Plans — Compute: most flexible (any family/region/OS); up to 66% off
- Savings Plans — EC2 Instance: specific family/region; up to 72% off
- Spot: up to 90% off; 2-min interruption warning; fault-tolerant only
- Dedicated Hosts: BYOL; physical server; socket/core licensing compliance
- Mixed Instances Policy: On-Demand base capacity + Spot for cost savings in ASG
- Convertible RIs: cannot be sold on Marketplace; exchange for equivalent value

Storage Optimization

- EBS gp3: set IOPS/throughput independently; ~20% cheaper than gp2 — prefer it
- EBS io2 Block Express: 256k IOPS, 4TB per volume — mission-critical databases
- S3 lifecycle: Standard → Standard-IA (30d min) → Glacier → Deep Archive
- S3 Intelligent-Tiering: auto-moves between tiers; no retrieval fee; small monthly fee
- S3 Glacier Deep Archive: cheapest; 12hr retrieval; for compliance archival
- EFS Lifecycle: auto-move to EFS-IA; per-request retrieval pricing

Networking Performance

- **Cluster PG**: same physical rack; lowest latency; for HPC/MPI tightly-coupled apps
- **Spread PG**: different hardware; max 7 instances/AZ; critical independent workloads
- **Partition PG**: separate racks per partition; Hadoop, Kafka, Cassandra
- **ENA**: Enhanced Networking; up to 100 Gbps; lower CPU overhead; free
- **EFA**: OS-bypass (RDMA-like); required for MPI & NCCL (ML training); HPC only
- Global Accelerator: TCP/UDP; static Anycast IPs; AWS backbone; no caching
- CloudFront: HTTP/S only; edge caching; OAC for S3; Lambda@Edge for logic
- GA vs CF: need static IPs or non-HTTP → GA; need caching or HTTPS → CF
- Local Zones: sub-10ms latency for city users; extend VPC to metro area
- Outposts: AWS rack on-premises; same APIs/console; consistent hybrid ops

Cost Visibility & Governance

- Cost Explorer: 13-month history; 12-month forecast; filter by tag/service/account
- CUR (Cost & Usage Report): most granular billing data → S3 → Athena/QuickSight
- Compute Optimizer: ML right-sizing; requires 14+ days CloudWatch utilization data
- Trusted Advisor: Business/Enterprise = all 5 category checks; Developer = core only
- Cost Allocation Tags: MUST ACTIVATE in Billing → Tags before they appear in CUR
- AWS Budgets: alert at forecast threshold; trigger actions (SCP, stop instances)

THE 7 Rs OF MIGRATION — COMPLETE REFERENCE

Strategy	Effort	Key AWS Tool(s)	Best For	Trade-off
Retire	None	—	Decommission unused apps (10–20% of portfolio)	No cost savings beyond switch-off
Retain	None	—	Compliance, not ready, or recently upgraded on-prem	Ongoing on-prem cost continues
Rehost	Low	AWS MGN	Fastest migration; lift-and-shift VMs with minimal changes	No cloud-native benefit; same architecture
Relocate	Low	VMware Cloud on AWS + HCX	Move VMware workloads; no agent; no OS changes required	VMware licensing cost on AWS infrastructure
Repurchase	Low-Med	SaaS (Salesforce, etc.)	Replace legacy app with SaaS; drop custom maintenance	Data migration to SaaS; retraining users
Replatform	Medium	RDS, Elastic Beanstalk	Minor optimizations; move to managed DB or PaaS runtime	Some refactoring needed; partial cloud benefit
Refactor	High	Lambda, ECS/EKS, Aurora	Maximum cloud benefit; redesign for microservices/serverless	Highest cost & time; needs app expertise

MASTER QUICK REFERENCE — KNOW THESE COLD

Service / Concept	Dom	The Key Fact to Remember
SCPs (Service Control Policies)	D1	Max permissions only — do NOT grant access. Management account IMMUNE. Deny wins always.
Control Tower Guardrails	D1	Preventive = SCPs | Detective = Config rules. Account Factory for new account vending.
RAM Shared Subnets	D1	Central networking; member accounts deploy workloads in shared subnets; one NAT GW shared.
Transit Gateway Route Tables	D1	Associate + Propagate per table. Segment prod/dev by blocking route propagation between TGWs.
IAM Identity Center	D1	Recommended for multi-account SSO. Connect IdP via SAML/SCIM. Permission Sets per account/OU.
Permission Boundaries	D1	Cap on max perms for IAM entities. Admin delegates identity creation safely to sub-admins.
External ID (cross-account roles)	D1	Prevents confused deputy attack. Third party provides External ID; you require it in trust policy.
Step Functions Standard vs Express	D2	Standard: 1-year, exactly-once, full audit. Express: 5-min, at-least-once, 100k events/sec.
SNS Fan-Out Pattern	D2	One SNS publish → multiple SQS queues. Each consumer independent. Resilient parallel processing.
Kinesis vs SQS	D2	Kinesis: ordered per shard, replay, streaming analytics. SQS: infinite scale, decouple, simple queue.
Aurora Global Database	D2	Multi-region active-passive. <1s RPO, ~1min RTO on promotion. One primary, up to 5 secondaries.
DynamoDB Global Tables	D2	Multi-region ACTIVE-ACTIVE. All replicas read & write. Last-writer-wins conflict resolution.
CloudFront OAC vs OAI	D2	OAC is the replacement for OAI. Supports SSE-KMS, POST/PUT, all S3 regions. Use OAC for new setups.
DR: Backup vs Pilot vs Warm vs Multi	D2	Cost/speed tradeoff: Backup(cheapest/slowest) → Pilot Light → Warm Standby → Multi-Site(best RTO/RPO)
MGN vs DMS	D3	MGN = server rehost (VM lift-and-shift). DMS = database migration with CDC. Different tools, different layers.
DMS + SCT (heterogeneous)	D3	Different DB engines: SCT first (converts schema/code), then DMS (migrates data + CDC replication).
DataSync vs Snowball	D3	DataSync = online, incremental, scheduled transfers. Snowball = offline, large one-time, poor WAN.
Spot Instances	D4	2-min interruption warning. Diversify instance types/AZs. Mixed Instances Policy in ASG. Fault-tolerant only.
EBS gp3 vs gp2	D4	gp3: set IOPS and throughput independently, ~20% cheaper. Always prefer gp3 for new volumes.
EFA vs ENA	D4	ENA = enhanced networking (100Gbps). EFA = OS-bypass for MPI/NCCL — required for HPC and ML training.
Global Accelerator vs CloudFront	D4	GA: TCP/UDP, static IPs, no caching. CF: HTTP/S, edge caching. Need static IPs or non-HTTP → use GA.
Cost Allocation Tags	D4	Must ACTIVATE in Billing & Cost Mgmt console. Applying tags to resources alone does NOT appear in CUR.
Compute Optimizer	D4	ML-powered right-sizing for EC2/Lambda/EBS/ECS. Requires 14+ days CloudWatch utilization metrics.

EXAM TIPS: 750/1000 to pass | 75 Qs | 180 min | No penalty for guessing | Mark & review unknown Qs

HOT TOPICS: SCPs skip mgmt account · TGW route table segmentation · MGN=rehost · SCT+DMS=heterogeneous DB

ALWAYS: RAM for shared subnets · EFA for HPC/MPI · gp3 over gp2 · Activate Cost Allocation Tags