

SAA-C03 // FINAL REVIEW GUIDE

01 // ACCESS + DATA SECURITY		02 // RESILIENCY + COMPUTE		03 // STORAGE + DATABASES		04 // CONSTANTS + EXAM TRAPS			
POLICY UNION	EVALUATION	EFFECTIVE PERMISSIONS		STORAGE S3	START WITH THE ACCESS MODEL		NUMBERS S3	CURRENT OFFICIAL LIMITS	
	Implicit deny. An applicable Allow is required. Identity and resource policies add permissions; an Allow in either can permit same-account access.		Regional object store with strong consistency, lifecycle, versioning and replication; not a POSIX file system.		Object max 48.8 TiB. Consider multipart at 100 MB; max 10,000 parts, normally 5 MiB-5 GiB each. [5]				
INTERSECT	Permissions boundary and SCP cap permissions. They do not grant access.		MULTI-REG	Use for Region-level DR, global latency, sovereignty, or multi-active requirements; replication is explicit.		S3 LIFE	Default lifecycle will not transition objects under 128 KB. Minimums: IA 30d; Glacier Instant/Flexible 90d; Deep Archive 180d.		
DENY	An explicit Deny in any applicable policy overrides an Allow. [2]		RTO	Maximum acceptable service-restoration delay after disruption.		EFS	Regional elastic NFS file system for shared Linux access across AZs; mount targets provide VPC access.		
ROLES	STS issues temporary credentials; federation maps external identities to roles. Protect root with MFA; prefer Identity Center for workforce.		RPO	Maximum acceptable time since the last recoverable data point - the tolerated data-loss window. [11]		FSX	Managed file systems: Windows/SMB+AD, Lustre/HPC+S3, NetApp ONTAP, or OpenZFS.		
CONTROL PLANE	KMS	// PICK THE RIGHT CONTROL	BACKUP	A backup is a recovery point; a replica is a live copy and can propagate deletion or corruption. Test restores.		HYBRID	Storage Gateway presents file/volume/tape; DataSync moves files and objects; Snow handles constrained or offline transfer.		
			PATTERN	Stateless tiers + health checks + Auto Scaling; make consumers idempotent; retry with backoff/jitter; isolate poison work in a DLQ.		S3 CLASS // ACCESS + RESILIENCY + MINIMUM			
SECRETS	Secrets Manager stores and rotates credentials; Parameter Store fits configuration and simpler secret use cases.		DR LADDER	// COST UP, RTO/RPO DOWN		STANDARD	Frequent or unknown hot access; multi-AZ; no minimum duration.		
TLS	ACM manages certificates for integrated AWS services. Use TLS in transit; KMS-backed encryption at rest.		BACKUP	Recreate and restore after disaster: lowest steady cost, longest recovery.		INTELLIG	Unknown/changing access; automatic tiers; monitoring fee; no retrieval fee.		
EDGE	WAF filters Layer 7 requests; Shield mitigates DDoS. GuardDuty detects threats; Macie discovers sensitive S3 data.		PILOT	Core data/services run; scale application capacity during recovery.		STD-IA	Infrequent but millisecond access; multi-AZ; retrieval fee; 30-day minimum.		
MODEL	AWS secures the cloud; customers secure identities, data, configuration, guest OS, and application choices.		WARM	Reduced but functional stack runs; scale it to production capacity.		1Z-IA	Recreateable infrequent data; one AZ; retrieval fee; 30-day minimum.		
VPC NETWORK INVARIANTS	PUBLIC	Subnet route to IGW. IPv4 internet access also needs a public IPv4/EIP and permissive SG/NACL.	ACTIVE	Full capacity in multiple sites/Regions: shortest recovery, highest cost and complexity.		GLACIER	Instant: milliseconds/90d. Flexible: minutes-hours/90d. Deep Archive: hours/180d. Restore archived objects first. [5]		
			COMPUTE + LOAD BALANCING		DATABASE // MODEL, ACCESS PATTERN, SCALE				
PRIVATE	No IGW route. Public NAT gateway sits in a public subnet with EIP; instances initiate outbound connections.		ALB	Layer 7 HTTP/HTTPS: host/path/header routing, redirects, WebSocket/gRPC, WAF integration.		RDS	Multi-AZ DB instance: synchronous HA standby, not read scale. Read replica: asynchronous read scale; promote for DR.		
SG	Stateful, allow-only, attached to ENIs/resources. Return traffic is automatically allowed.		NLB	Layer 4 TCP/UDP/TLS: extreme throughput, source IP preservation, static IP/EIP per enabled AZ.		AURORA	MySQL/PostgreSQL-compatible distributed storage, fast replicas, Serverless; Global Database for cross-Region reads/DR.		
NACL	Stateless, ordered allow/deny rules at subnet boundary. Configure both directions and ephemeral ports.		GWLb	Layer 3 virtual appliances; transparent flows over GENEVE port 6081. [4]		DYNAMO	Key-value/document at scale. Design partition/sort keys for access patterns; avoid hot keys and scans.		
ROUTES	Longest prefix wins; for an identical destination, a static route beats a propagated route. [3]		EC2	Choose for OS control, custom runtimes, steady/long processes, or specialized instances.		INDEX	GSI: alternate partition key, create later, eventual reads. LSI: same partition key, create with table, strong reads possible, 10 GiB item collection.		
ENDPOINT	Gateway: S3/DynamoDB, route tables, no added endpoint charge. Interface: PrivateLink ENIs, DNS, SGs, hourly/data cost.		LAMBDA	Event-driven, short-lived, stateless compute; scale concurrency and design for retries.		CACHE	DAX caches DynamoDB reads. ElastiCache offloads hot reads/session data; a cache is not the source of record.		
CONNECT	Peering is one-to-one and non-transitive; Transit Gateway is hub-and-spoke. VPN is IPsec; DX is dedicated private connectivity.		CONTAINER	Fargate removes host management; ECS is AWS-native orchestration; EKS is managed Kubernetes.		ANALYTIC	Redshift is an OLAP warehouse; Athena runs serverless SQL over S3; OpenSearch serves search/log analytics.		
BUFFER + FANOUT	SQS	Pull buffer/backpressure. Standard: at-least-once, best-effort order. FIFO: ordered and deduplicated per group.	DECOUPLE // MESSAGE, EVENT, OR WORKFLOW		EDGE + GLOBAL DELIVERY				
			EVENT	EventBridge filters/routes events from AWS, custom apps, and SaaS; rules send matching events to targets.		DNS/CDN	Route 53 supplies DNS, health checks, and routing. CloudFront caches HTTP at edge and integrates with WAF; neither replicates application state.		
			STREAM	Kinesis retains ordered records in shards for replay and multiple consumers; partition key selects the shard.		GLOBAL	Global Accelerator gives static anycast IPs and optimizes TCP/UDP paths; S3 Transfer Acceleration targets S3 uploads.		
			FLOW	Step Functions provides durable state, sequencing, branching, retries, and callbacks. API Gateway fronts HTTP/REST/WebSocket APIs.					
ABBREVIATIONS			SG security group NACL network access control list			ALB Application Load Balancer NLB Network Load Balancer			
AZ Availability Zone HA high availability			ENI Elastic Network Interface EIP Elastic IP			GWLb Gateway Load Balancer			
FT fault tolerance RPO recovery point objective			IGW internet gateway NAT Network Address Translation			EBS Elastic Block Store EFS Elastic File System			
RTO recovery time objective			VGV virtual private gateway TGW transit gateway			FSX managed file systems RDS Relational Database Service			
IAM Identity and Access Management			DX Direct Connect			GSI global secondary index LSI local secondary index DAX DynamoDB Accelerator			
STS Security Token Service SCP service control policy						SQS Simple Queue Service SNS Simple Notification Service			
						FIFO first in, first out DLQ dead-letter queue			
						KMS Key Management Service ACM Certificate Manager			
						WAF Web Application Firewall			
						RCU read capacity unit WCU write capacity unit			