AWS CERTIFIED · SOA-C02

SysOps Administrator Associate

QUICK REFERENCE CHEAT SHEET

65+20	130	720	6
Scored+Unscored	Minutes	Pass Score	Domains

D1 · Monitoring & Logging	D2 · Reliability	D3 · Deployment	D4 · Security	D5 · Networking	D6 · Cost & Perf
20%	16%	18%	16%	18%	12%

| DOMAIN 1 · MONITORING, LOGGING & REMEDIATION (20%)

CloudWatch Metrics

- Default EC2: CPU, Network, Disk I/O — **NOT memory or disk space**
- Install CloudWatch Agent for memory, disk, custom OS metrics
- Detailed monitoring: 1-min (default: 5-min) — enable per instance
- Custom metrics: PutMetricData API with custom Namespace
- High-resolution custom: 1-second granularity
- Retention: 15 months (granularity reduces over time)

CloudWatch Alarms

- States: OK | ALARM | INSUFFICIENT_DATA (not an error — no data)
- INSUFFICIENT_DATA: evaluation period has no data points
- Composite Alarms: AND/OR logic — reduce alert noise
- Actions: SNS, EC2 action, ASG scaling, SSM OpsCenter

CloudWatch Logs

- Log Groups → Log Streams → Log Events
- Metric Filters: create CW metrics from log patterns
- Log Insights: SQL-like queries across log groups
- Subscription Filters: stream to Lambda/Kinesis/Firehose real-time
- Retention: 1 day to never — set per log group
- Export to S3: CreateExportTask (async)

AWS CloudTrail

- "Who called what API" — records all API activity
- Management Events: default on (CreateBucket, RunInstances)
- Data Events: S3 object-level, Lambda invocations — off by default
- Insight Events: detect unusual API call patterns
- Log file validation: SHA-256 — enable for integrity
- Multi-region trails: default for new trails

AWS Config

- Records resource configuration changes over time
- Config Rules: evaluate compliance (managed or custom Lambda)
- Auto-remediation: non-compliant → trigger SSM Automation
- Aggregator: multi-account, multi-region compliance view
- Conformance Pack: bundle of Config rules + remediation
- Config ≠ CloudTrail: Config = state, CloudTrail = API calls

EventBridge Schedules

- rate(5 minutes) | rate(1 hour) — simple intervals
- cron(minute hour dom month dow year)
- Daily 8AM UTC: cron(0 8 * * ? *)
- Weekdays noon: cron(0 12 ? * MON-FRI *)
- ? required in dom OR dow (not both)

Service	What It Tracks	Key Use Case	Exam Tip
CloudWatch Metrics	Performance over time	Auto Scaling, alarms	Memory needs CW Agent
CloudWatch Logs	Log data from apps/OS	Pattern match, alerting	Metric Filters create metrics
CloudTrail	API call history	Security audit, compliance	Data Events off by default
AWS Config	Resource config state	Compliance, drift detect	Auto-remediate via SSM
EventBridge	Events from AWS services	Trigger Lambda/workflows	cron(0 8 * * ? *)

| DOMAIN 2 · RELIABILITY & BUSINESS CONTINUITY (16%)

EC2 Auto Scaling

- Policies: Target Tracking (simplest), Step, Scheduled
- Cooldown (default 300s): prevents rapid scale cycles (thrashing)
- Lifecycle Hooks: pause on launch/terminate for custom actions
- Warm Pool: pre-initialized stopped instances for fast scale-out
- Default termination: oldest launch config in most-populated AZ

Elastic Load Balancing

- ALB: Layer 7, path/host routing, WebSocket, Lambda targets
- NLB: Layer 4, static IP, ultra-low latency, TCP/UDP/TLS
- GWLB: Layer 3, bump-in-the-wire for security appliances (NFW)
- CLB: legacy, avoid for new deployments
- Deregistration Delay (ALB/NLB): 300s — lets in-flight complete
- Cross-Zone LB: distribute evenly across all AZs

Route 53 Health Checks

- HTTP/HTTPS/TCP probes — 30s (fast: 10s)
- Calculated: combine multiple checks with AND/OR
- CloudWatch alarm-based: for private VPC endpoints
- Failover: primary (with health check) → secondary on failure
- DNS CNAME auto-updates on RDS Multi-AZ failover

RDS High Availability

- Multi-AZ: synchronous standby, auto failover ~1-2 min
- Standby NOT accessible for reads — only for failover
- Read Replicas: async, for read scaling, cross-region possible
- Multi-AZ DB Cluster: up to 2 standbys, can serve reads
- Automated backups: 1-35 days, PITR supported

S3 Resilience

- 11 nines durability — data across 3+ AZs
- Versioning: delete marker instead of delete; recover by deleting marker
- MFA Delete: require MFA for version deletion
- CRR (Cross-Region Replication): async to another region
- SRR (Same-Region): for log aggregation, compliance copies
- Existing objects NOT replicated by CRR — use S3 Batch Ops

AWS Backup

- Centralized backup: EC2, EBS, RDS, DDB, EFS, S3
- Backup Plans: schedules, lifecycle, retention policies
- Vault Lock (Compliance): WORM — even root cannot delete
- Vault Lock (Governance): admins with permission can remove
- Cross-region and cross-account copies supported

DR Strategy	RTO	RPO	Cost	Description
Backup & Restore	Hours	Hours	$	Restore from backups/snapshots in new region
Pilot Light	~10 min	Minutes	$$	Core services running; scale out on failover
Warm Standby	Minutes	Seconds	$$$	Scaled-down full copy; scale up on failover
Multi-Site Active/Active	~0	~0	$$$$	Full capacity in multiple regions simultaneously

| DOMAIN 3 · DEPLOYMENT, PROVISIONING & AUTOMATION (18%)

CloudFormation

- Change Sets: preview ADD/MODIFY/REMOVE before applying
- Drift Detection: find resources changed outside CFN
- StackSets: deploy across multiple accounts + regions
- Nested Stacks: reuse common patterns as child stacks
- DeletionPolicy: Retain (keep), Snapshot (for RDS/EBS)
- cfn-signal + CreationPolicy: wait for bootstrap before complete
- cfn-hup: detect metadata changes on running instances
- ContinueUpdateRollback: fix UPDATE_ROLLBACK_FAILED state

EC2 Image Builder

- Automates AMI/container image build, test, distribute
- Recipe: base OS + build components + test components
- Image Pipeline: scheduled or on-demand builds
- Cross-region, cross-account distribution
- SSM Parameter Store: share latest AMI IDs

AWS Systems Manager

- Run Command: scripts on fleets without SSH/RDP
- Session Manager: browser SSH/RDP, no bastion, CloudTrail logged
- Patch Manager: baselines + patch groups + maintenance windows
- Automation: runbooks (SSM Documents) for auto-remediation
- Parameter Store: config values (SecureString via KMS)
- Inventory: collect metadata from managed instances
- Prerequisite: SSM Agent + AmazonSSMManagedInstanceCore role
- Private subnet SSM: need 3 VPC Interface Endpoints

Elastic Beanstalk

- All at Once: fastest, brief downtime possible
- Rolling: gradual, reduced capacity during update
- Rolling+Batch: full capacity maintained throughout
- Immutable: new ASG, zero downtime, instant rollback — safest
- Blue/Green: CNAME swap, zero downtime, instant DNS rollback
- .ebextensions/: YAML config for packages, files, commands

SSM Feature	Purpose	Key Detail
Run Command	Run scripts at scale	No SSH; output to S3/CloudWatch Logs
Patch Manager	OS patching	Baseline + Patch Group + Maintenance Window
Session Manager	Secure shell access	No bastion; logged to CloudTrail
Automation	Run runbooks	Used for Config auto-remediation
Parameter Store	Config/secrets	SecureString = KMS encrypted
Inventory	Asset tracking	Software, patches, network config metadata

| DOMAIN 4 · SECURITY & COMPLIANCE (16%)

IAM Policy Evaluation

- Explicit Deny > Allow > Implicit Deny — always
- SCPs: restrict max permissions for OUs/accounts (org-wide)
- SCPs do NOT apply to management (root) account
- Permission Boundaries: max for IAM entity — do not grant
- Cross-account: both identity AND resource policy must allow

KMS & Encryption

- KMS max direct encrypt: 4 KB — use envelope for larger data
- Envelope: GenerateDataKey → encrypt locally → store enc. DEK
- All KMS API calls logged in CloudTrail
- AWS Managed Keys: auto-rotated annually, free
- Customer Managed Keys (CMK): full control, manual or auto rotate
- Multi-Region Keys: replicate key material cross-region

Shield & WAF

- Shield Standard: free, L3/L4 DDoS auto-protection
- Shield Advanced: $3K/month, L7, DRT access, cost protection
- WAF: attach to CloudFront, ALB, API GW, AppSync
- WAF rules: IP/geo match, rate-based, managed OWASP groups

Threat Detection Suite

- GuardDuty: threat detection ML on VPC Flow + CloudTrail + DNS
- Inspector v2: CVE scanning on EC2 (via SSM), ECR, Lambda
- Macie: sensitive data (PII, credentials) in S3 via ML
- Security Hub: aggregates findings from all above + Config
- Security Hub requires: AWS Config enabled in all accounts
- All findings → EventBridge for automated response

Secrets Manager vs SSM Param Store

- Secrets Manager: auto-rotation, $0.40/secret/month, 64 KB
- SSM Standard: free, 4 KB, no native rotation
- SSM Advanced: paid, 8 KB, TTL policies
- Use Secrets Manager for DB passwords needing rotation
- Use SSM for non-rotating config: endpoints, feature flags

AWS Organizations

- SCPs set max permissions — do NOT grant access
- Consolidated Billing: volume discounts across accounts
- Tag Policies: enforce consistent resource tagging
- Backup Policies: enforce backup plans across org
- CloudTrail org trail: logs all accounts to central S3

| DOMAIN 5 · NETWORKING & CONTENT DELIVERY (18%)

VPC Fundamentals

- IGW: internet access for public subnets
- NAT GW: private subnet outbound internet (place in public subnet)
- Egress-Only IGW: IPv6-only outbound for private subnets
- Security Groups: stateful, instance-level, allow rules only
- NACLs: stateless, subnet-level, allow + deny, numbered priority
- NACLs: allow ephemeral ports 1024-65535 for responses (stateless!)
- VPC Flow Logs: captures ACCEPT/REJECT metadata, not payload

VPC Connectivity

- VPC Peering: two VPCs direct, NON-transitive
- Transit Gateway: hub-and-spoke, transitive, scales to 1000s of VPCs
- Gateway Endpoint: FREE, S3 + DynamoDB only, route table based
- Interface Endpoint: most AWS services, ENI, hourly cost, private DNS
- PrivateLink: expose services privately to other VPCs

Hybrid Connectivity

- Site-to-Site VPN: encrypted over internet, quick setup, up to 1.25G
- Direct Connect: dedicated private, consistent latency, 1-100 Gbps
- DX lead time: weeks to months for physical provisioning
- DX + VPN: use VPN as backup/failover for Direct Connect
- DX Gateway: access multiple VPCs/regions from one DX connection
- VPN CloudHub: hub-and-spoke VPN across multiple customer sites

CloudFront & Route 53

- CloudFront OAC: restrict S3 to CloudFront only (replaces OAI)
- Invalidation: immediately purge files from edge caches
- Signed URLs/Cookies: restrict content to authenticated users
- Lambda@Edge: run code at CloudFront edge locations
- Route 53 Alias: free, point to AWS resources (no IP needed)
- CNAME: cannot use at zone apex (use Alias instead)
- Private Hosted Zone: requires enableDnsSupport + enableDnsHostnames

Connectivity	Use Case	Cost	Notes
VPC Peering	2 VPCs, same/cross-account	Free within region	Non-transitive; no overlapping CIDRs
Transit Gateway	Many VPCs + on-prem hub	Per attachment + data	Transitive; supports VPN/DX attachments

Gateway Endpoint	S3 and DynamoDB only	Free	Update route table; no DNS needed
Interface Endpoint	Most AWS services	Hourly + data	ENI; needs enableDnsSupport = true
Site-to-Site VPN	On-prem to AWS (fast)	Low	Over internet; variable latency
Direct Connect	On-prem to AWS (reliable)	High + NRC	Weeks to provision; dedicated circuit

| DOMAIN 6 · COST & PERFORMANCE OPTIMIZATION (12%)

Cost Management Tools

- Cost Explorer: visualize 12 months, forecast, filter by tag/service
- AWS Budgets: alerts on cost/usage/RI/Savings Plans thresholds
- CUR (Cost & Usage Report): most detailed → S3 → Athena/QuickSight
- Cost Allocation Tags: activate in Billing console (required step!)
- Compute Optimizer: ML right-sizing (needs 30 days CW data)
- Trusted Advisor: 5 pillars; full checks require Business/Enterprise

Purchasing Options

- On-Demand: no commitment, highest cost
- Reserved Instances: 1/3 yr, up to 72% off, Standard or Convertible
- Savings Plans: Compute (most flexible) or EC2 Instance, hourly commitment
- Spot: up to 90% off, 2-min interruption notice, for fault-tolerant workloads
- Dedicated Hosts: BYOL, physical server visibility, compliance
- Convertible RIs: cannot sell on RI Marketplace (Standard RIs can)

S3 Storage Classes

- Standard: frequent, ms latency, 3 AZs
- Standard-IA: infrequent, retrieval fee, min 30 days
- One Zone-IA: single AZ, 20% cheaper than Std-IA
- Glacier Instant: archive, ms retrieval, min 90 days
- Glacier Flexible: minutes-hours retrieval, min 90 days
- Glacier Deep Archive: cheapest, 12h retrieval, min 180 days
- Intelligent-Tiering: auto-moves tiers, no retrieval fee
- Lifecycle Policy: automate transitions and expiration

EC2 Performance

- EBS gp3: preferred over gp2 — independent IOPS/throughput, cheaper
- EBS-Optimized: dedicated EC2 to EBS bandwidth
- Enhanced Networking (ENA): up to 100 Gbps, lower latency
- Cluster PG: same rack, lowest latency for HPC
- Spread PG: separate hardware, max 7 per AZ
- Partition PG: HDFS/Kafka, racks as partitions

| MASTER QUICK REFERENCE — KNOW THESE COLD

Service / Concept	Domain	Remember This
CloudWatch Agent	D1	Required for memory/disk metrics — install via SSM Run Command
INSUFFICIENT_DATA	D1	Not an error — means no metric data in evaluation period
CloudTrail Data Events	D1	S3 object-level + Lambda invocations — disabled by default, extra cost
Config vs CloudTrail	D1	Config = what state is resource. CloudTrail = who made API call
Config Auto-Remediation	D1	Non-compliant resource → trigger SSM Automation runbook
EventBridge Cron	D1	cron(minute hour dom month dow year) — ? in dom OR dow, not both
Auto Scaling Cooldown	D2	300s default — prevents thrashing (rapid scale-out/in cycles)
RDS Multi-AZ	D2	Sync standby, auto-failover, CNAME updates auto — NOT for reads
RDS Read Replica	D2	Async, for read scaling, promotable — NOT HA (no auto-failover)
S3 Delete Marker	D2	Versioning: delete inserts marker. Recover = delete the marker
S3 CRR + existing objects	D2	CRR only replicates NEW objects. Use S3 Batch Ops for existing
Backup Vault Lock Compliance	D2	WORM — even root cannot delete backups during retention period
CFN Change Sets	D3	Preview ADD/MODIFY/REMOVE before applying — required in production
CFN DeletionPolicy	D3	Retain: keep resource when stack deleted. Snapshot: take snapshot first
SSM private subnet	D3	Need 3 Interface Endpoints: ssm, ssmmessages, ec2messages

EB Immutable	D3	New ASG, zero downtime, safest, instant rollback: terminate new ASG
Explicit Deny	D4	ALWAYS wins — no Allow can override an explicit Deny in IAM
SCPs + management account	D4	SCPs do NOT apply to the management (root/master) account
KMS 4KB limit	D4	Use envelope encryption: GenerateDataKey → encrypt locally
Secrets Manager vs SSM	D4	Secrets Manager = auto-rotation. SSM = free, non-rotating config
GuardDuty data sources	D4	VPC Flow Logs + CloudTrail Events + DNS Logs
Security Hub requirement	D4	Requires AWS Config enabled in all member accounts
NAT GW placement	D5	Deploy in PUBLIC subnet; add route 0.0.0.0/0 → NAT GW from private
SG vs NACL stateless	D5	NACL is stateless — allow ephemeral ports 1024-65535 for responses
VPC Peering vs TGW	D5	Peering = non-transitive between 2. TGW = hub-spoke, transitive, many
Gateway vs Interface Endpoint	D5	Gateway: free, S3+DDB only, route table. Interface: hourly, most svcs, ENI
CloudFront Invalidation	D5	Immediately purge files from all edge caches — use /* for all
Route 53 Alias	D5	Free, can use at zone apex, points to AWS resources (ELB, CF, S3)
Cost Allocation Tags	D6	Must ACTIVATE in Billing console — applying tags alone is not enough
Compute Optimizer	D6	Needs 30 days CloudWatch data for EC2/EBS/Lambda right-sizing
Spot Interruption	D6	2-minute warning before interruption. Use for fault-tolerant workloads
gp3 vs gp2	D6	gp3: independent IOPS/throughput, cheaper — prefer for new volumes

- 720/1000 to pass | 65 scored + 20 unscored | 130 minutes | No penalty for guessing
- Unique to SOA-C02: Hands-on exam LAB component — practice in the AWS console!
- CW Agent for memory/disk | Config Rules + SSM for auto-remediation | CloudTrail Data Events = off by default
- Multi-AZ = sync HA, no reads | Read Replica = async reads, promotable | S3 CRR = new objects only
- CFN Change Sets before every prod update | DeletionPolicy: Retain for stateful resources
- Explicit Deny always wins | SCPs skip management account | Envelope encryption for data > 4KB
- NAT GW in public subnet | NACL stateless = allow ephemeral ports | TGW for many VPCs (transitive)
- Activate Cost Allocation Tags in Billing console | Compute Optimizer needs 30 days of CW data