AWS Certified Solutions Architect - Associate Cheat Sheet

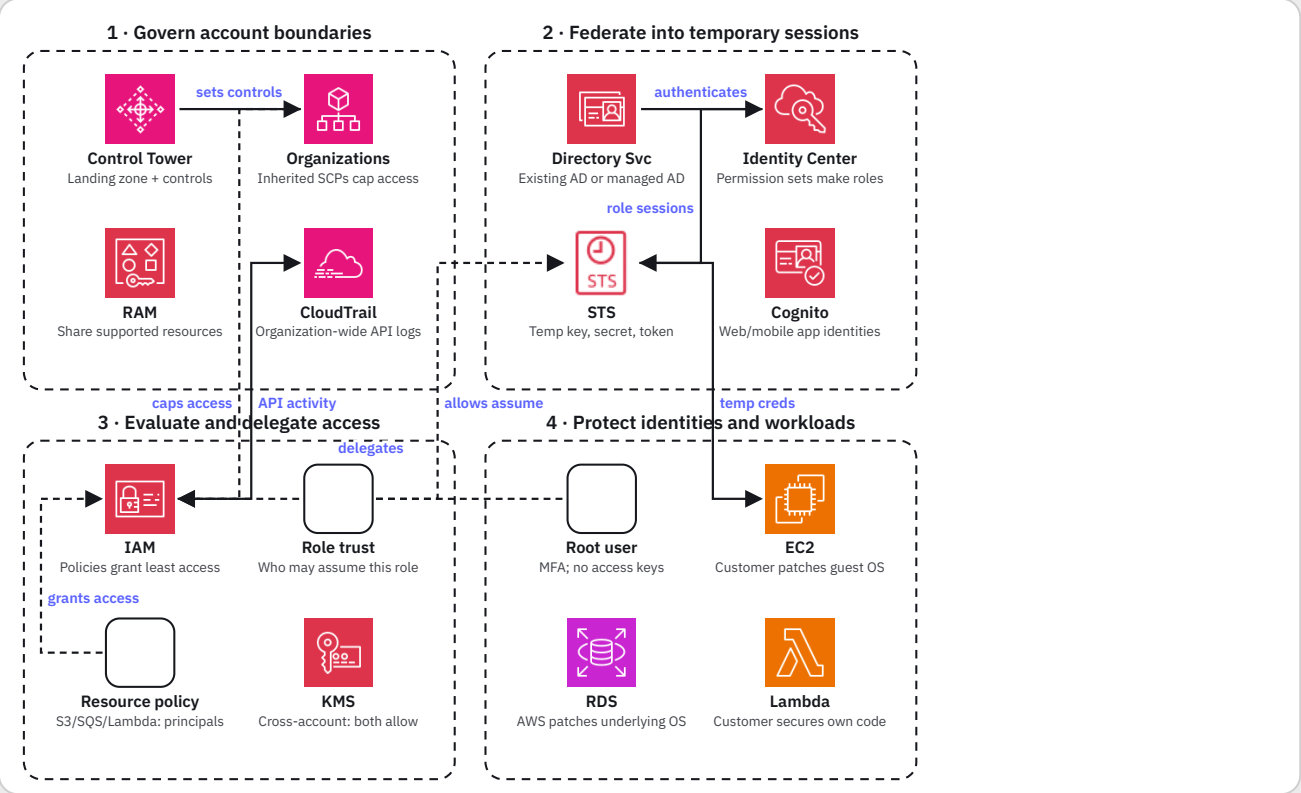
SAA-C03 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SECURE ARCHITECTURES · 30% OF THE EXAM · TASK STATEMENT 1.1

Design secure access to AWS resources

Govern, federate, authorize, protect



1 Govern account boundaries

Use **separate accounts** to limit blast radius and separate duties. Control Tower establishes governance; SCPs impose inherited ceilings. RAM shares resources without moving them; CloudTrail records activity, not enforcement.

2 Federate into temporary sessions

Use **IAM Identity Center** for workforce multi-account access; Directory Service connects existing AD. STS provides expiring role credentials. Cognito serves application users rather than governing workforce account access.

3 Evaluate and delegate access

Cross-account roles need caller permission plus target-role trust; role policies grant actions. Resource policies grant access to principals. Cross-account KMS requires caller IAM permission and key-policy authorization.

4 Protect identities and workloads

With **managed services**, AWS handles more infrastructure, not customer data or IAM duties. Reserve root for root-only tasks; prefer roles over keys. Residency includes replicas, backups and logs; AZs isolate failures within Regions.

Exam traps

- An **SCP grants no permissions**: it caps member-account access and inherits through the organization root and OUs. It does not restrict the management account; an applicable Allow is still required.
- An **explicit deny wins** over allows in applicable policies. Permission boundaries grant nothing. Groups organize IAM users; RBAC assigns roles; ABAC uses trusted principal and resource attributes.
- Prevent a **confused deputy** with ExternalId for third-party AssumeRole, or aws:SourceArn/SourceAccount for supported service access. MFA does not make long-lived workload keys the preferred choice.

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

AWS Certified Solutions Architect - Associate Cheat Sheet

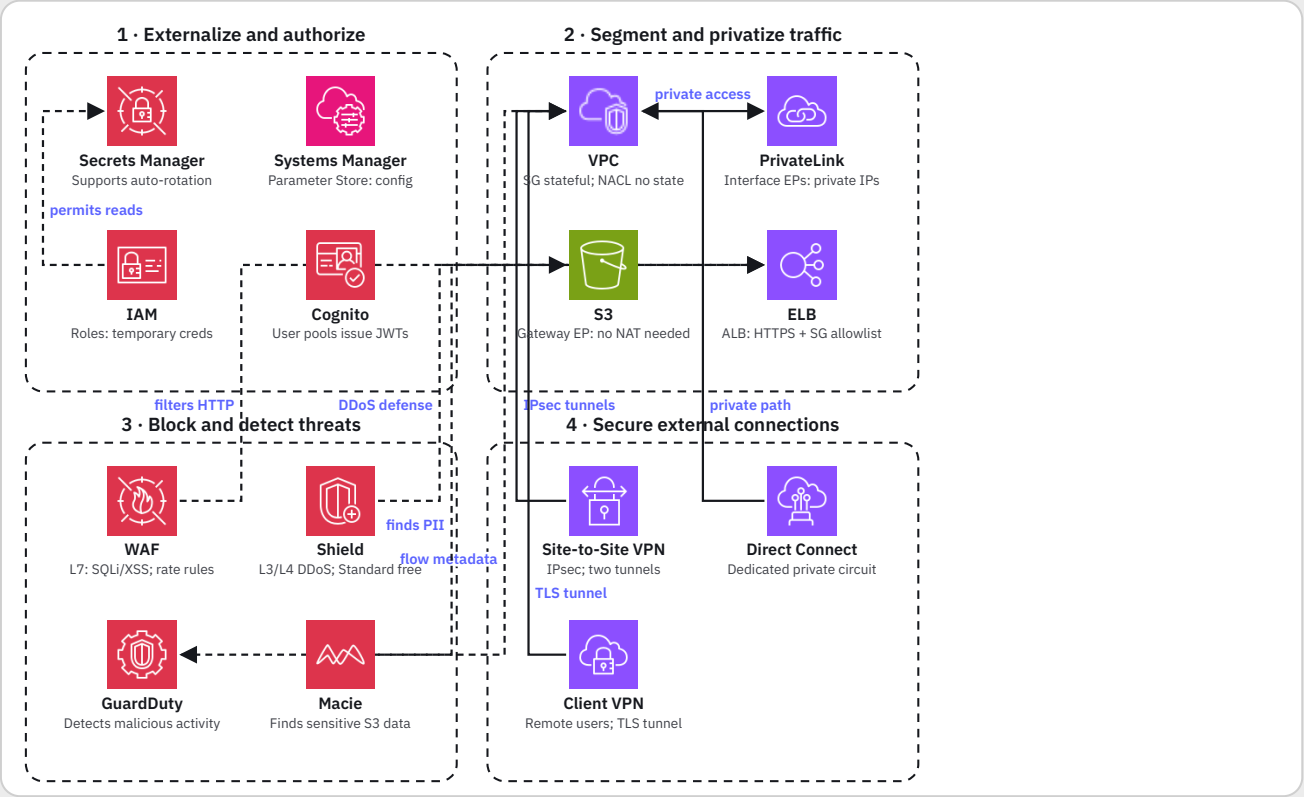
SAA-C03 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SECURE ARCHITECTURES · TASK STATEMENT 1.2

Design secure workloads and applications

Externalize, isolate, defend, connect



1 Externalize and authorize

Rotate secrets with Secrets Manager; Parameter Store fits configuration/SecureString without built-in rotation. IAM roles supply temporary workload credentials; Cognito identity pools supply AWS credentials.

2 Segment and privatize traffic

Private subnets lack a direct internet gateway route; NAT enables outbound IPv4, not unsolicited inbound access. S3 gateway endpoints use routes; interface endpoints use private IPs and security groups.

3 Block and detect threats

Detect ≠ prevent: GuardDuty flags threats; Macie finds sensitive S3 data. WAF blocks L7 SQLi/XSS with matching rules; Shield mitigates L3/L4 DDoS. Neither detector automatically blocks traffic.

4 Secure external connections

Encryption required: Site-to-Site VPN provides IPsec over internet; Direct Connect supplies dedicated connectivity, not default encryption. VPN over Direct Connect adds IPsec; Client VPN connects individual users.

Exam traps

- **Different findings**: Amazon Inspector finds software vulnerabilities; Amazon GuardDuty detects threats; Amazon Macie discovers sensitive S3 data. AWS Security Hub aggregates findings.
- **Customer vs workforce**: Amazon Cognito serves application users; AWS IAM Identity Center (AWS Single Sign-On) provides workforce access to AWS accounts and business applications.
- **Security groups allow only** and track return traffic. Network ACLs use ordered allow/deny rules and are stateless; omitting return ephemeral ports breaks connections.

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

AWS Certified Solutions Architect - Associate Cheat Sheet

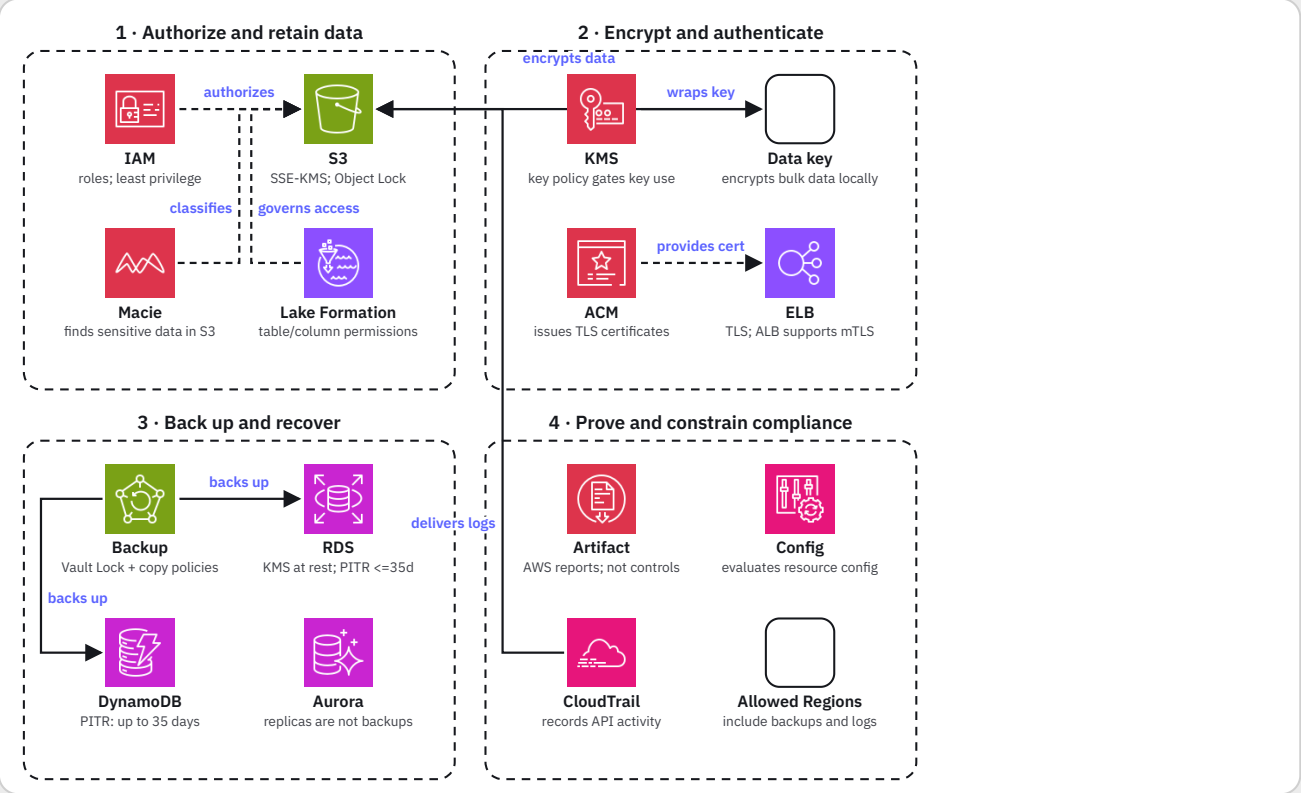
SAA-C03 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SECURE ARCHITECTURES · TASK STATEMENT 1.3

Determine appropriate data security controls

Authorize, encrypt, recover, prove



1 Authorize and retain data

Choose **Object Lock** for immutable versions: compliance retention cannot be shortened; legal holds last until removed. Lifecycle transitions reduce storage cost; classification guides access and retention.

2 Encrypt and authenticate

Choose **SSE-KMS** for managed key controls; client-side encryption sends ciphertext. Envelope encryption wraps data keys. TLS must protect each hop; ACM auto-renews eligible deployed certificates, not imported ones.

3 Back up and recover

RPO limits tolerable data loss; RTO limits recovery time. Choose backup frequency and restore methods accordingly. Cross-account copies isolate backups; protected keys, retention, and restore tests remain necessary.

4 Prove and constrain compliance

Data residency covers primary data, replicas, backups, and logs—not just the deployment Region. AWS supplies infrastructure assurances; customers configure data controls and retain evidence.

Exam traps

- **Cross-account SSE-KMS reads** need S3 authorization plus caller IAM permission and authorization in the KMS key policy. An S3 bucket-policy allow alone is insufficient.
- **Replication is not backup**: replicas can propagate accidental changes or deletions. Multi-AZ targets availability; retained backups and PITR recover earlier data states.
- **Key rotation** does not re-encrypt existing data; KMS retains old material for decryption. Key administration does not inherently grant permission to decrypt.

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

AWS Certified Solutions Architect - Associate Cheat Sheet

SAA-C03 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SECURE ARCHITECTURES · WHAT TO REMEMBER

Concepts and services of Design Secure Architectures

Concepts to know

Least privilege

Permissions allow only required actions on required resources under required conditions. Choose **scoped roles with temporary credentials** over shared users, embedded access keys, or broad administrative permissions.

Stateful and Stateless Filtering

Security groups are stateful, allow-only resource controls; network ACLs are stateless subnet controls with allow and deny rules. Choose **network ACLs for explicit subnet-level denies**; permit return traffic and ephemeral ports explicitly.

Encryption

Encryption protects confidentiality, not authorization or recoverability. Choose **separate controls for data at rest and in transit**; access to encrypted data can require both resource permissions and permission to use its encryption key.

Core services



AWS Identity and Access Management (IAM)

Choose **roles for workloads and cross-account access**, not shared access keys. Cross-account role assumption requires caller authorization and a role trust policy; applicable explicit denies override.



AWS Key Management Service (AWS KMS)

Choose **customer managed keys** for key-policy control and cross-account sharing. Automatic rotation preserves older key material for decryption; it does not re-encrypt existing data.



Amazon S3

Choose **Object Lock for immutable retention**, bucket policies for resource-level access, and Block Public Access to prevent public exposure. Versioning supports recovery but does not prevent deletion.

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