AWS Certified CloudOps Engineer - Associate Cheat Sheet

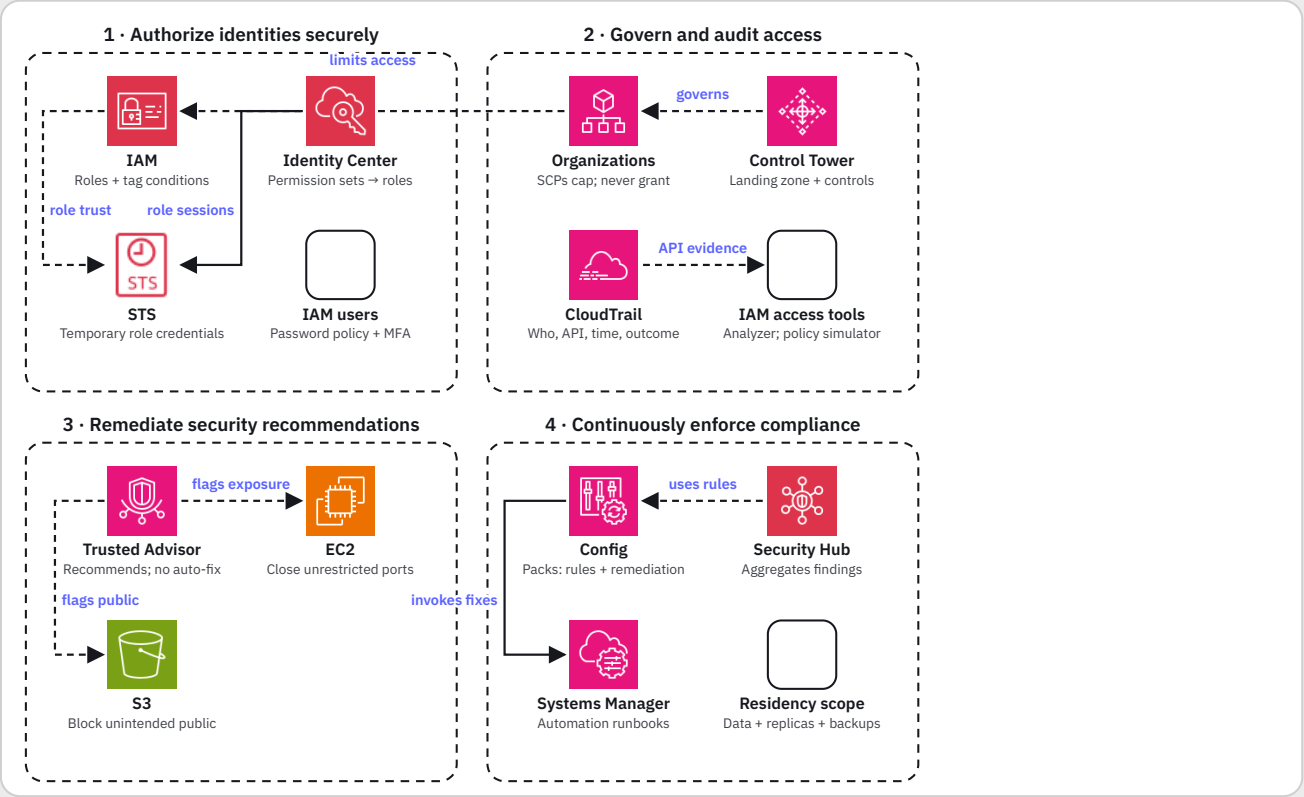
SOA-C03 · Domain 4 of 5

BlowStack

DOMAIN 4 · SECURITY AND COMPLIANCE · 16% OF THE EXAM · TASK STATEMENT 4.1

Implement and manage security and compliance tools and policies

Authorize, govern, remediate, monitor



1 Authorize identities securely

Use **roles + federation** for temporary, least-privilege access. RBAC assigns roles; ABAC matches trusted tags. Cross-account role assumption needs caller permission and role trust; resource policies can grant access directly.

2 Govern and audit access

Use **CloudTrail** for denied API context, policy simulator for policy evaluation, and IAM Access Analyzer for external/unused access. SCPs inherit root → OU → account; separate accounts reduce blast radius.

3 Remediate security recommendations

For **Trusted Advisor security findings**, restrict exposed ports, block unintended S3 access, and rotate/remove exposed or unused IAM keys. Apply fixes in the affected service, then refresh checks.

4 Continuously enforce compliance

Use **Config conformance packs** for organization-wide drift checks and optional remediation. Customer compliance also requires approved services/Regions and residency checks covering replicas, backups, and logs.

Exam traps

- **SCPs never grant access**; they cap member-account principals, including root, not management-account principals. Any applicable explicit deny overrides an allow.
- **IAM password policies** apply to IAM users, not federated passwords, which follow the identity source. Password policies do not enforce MFA; configure MFA separately.
- **Detection is not remediation**: Trusted Advisor recommends fixes; Config rules evaluate compliance. Automatic fixes require configured remediation, such as Systems Manager Automation.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate

AWS Certified CloudOps Engineer - Associate Cheat Sheet

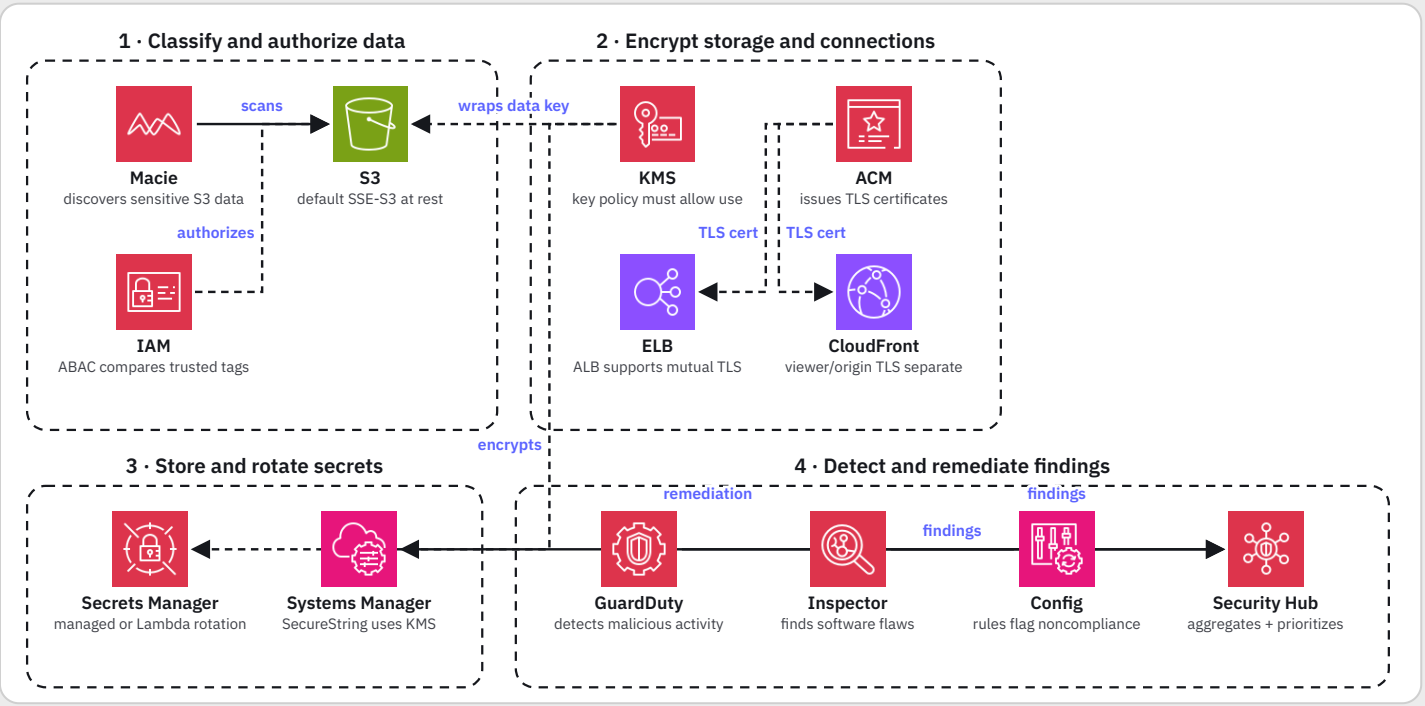
SOA-C03 · Domain 4 of 5

BlowStack

DOMAIN 4 · SECURITY AND COMPLIANCE · TASK STATEMENT 4.2

Implement strategies to protect data and infrastructure

Classify, encrypt, rotate, remediate



1 Classify and authorize data

Classification drives access, retention, and monitoring. Macie discovers sensitive S3 data; it does not enforce access. IAM ABAC uses principal/resource attributes; restrict who can change authorization tags.

2 Encrypt storage and connections

For **TLS certificates**, ACM must match the load balancer's Region; CloudFront requires us-east-1. EBS, RDS, and EFS support KMS encryption at rest. Certificate trust, hostname, and expiry affect TLS validation.

3 Store and rotate secrets

Choose Secrets Manager for **credential rotation** that coordinates secret and target updates. Parameter Store SecureString encrypts values but has no built-in credential rotation. Consumers must retrieve refreshed credentials.

4 Detect and remediate findings

Findings are not fixes: Security Hub consolidates findings; Config can invoke Systems Manager Automation for remediation. AWS Security Agent reviews application artifacts and tests running applications.

Exam traps

- **Envelope encryption** encrypts data locally with a data key; KMS protects that key. KMS rotation retains old key material; it neither re-encrypts stored data nor rotates passwords.
- **Encryption defaults** do not fix existing data: encrypt EBS snapshot copies and create volumes, restore RDS from an encrypted snapshot copy, and migrate files to a new encrypted EFS file system.
- **TLS termination** protects only that connection; use HTTPS to targets to encrypt the next hop. Mutual TLS authenticates clients but does not replace application authorization.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate

AWS Certified CloudOps Engineer - Associate Cheat Sheet

SOA-C03 · Domain 4 of 5

BlowStack

DOMAIN 4 · SECURITY AND COMPLIANCE · WHAT TO REMEMBER

Concepts and services of Security and Compliance

Concepts to know

Effective Permissions

Authorization combines identity and resource policies with applicable permission ceilings and request conditions. **An explicit deny wins**; adding an allow cannot override it, and service control policies do not grant permissions.

Encryption at Rest

Stored data is protected by encryption and key controls. Troubleshooting requires checking **data permissions and key permissions**; rotating key material does not re-encrypt existing data.

Encryption in Transit

TLS protects traffic between communicating endpoints. **Evaluate every network hop**: an HTTPS listener does not ensure encrypted backend connections, and mutual TLS additionally authenticates clients with certificates.

Core services



AWS Identity and Access Management (IAM)

Use **roles for temporary access**, policies for authorization, and conditions to constrain requests. Policy simulation tests authorization; Access Analyzer identifies external access and unused access.



AWS Key Management Service (AWS KMS)

Use customer managed keys when explicit key-policy, rotation, or cross-account controls are required. **Cross-account use requires authorization in both accounts**; an identity-policy allow alone fails.



AWS Config

Use **rules and conformance packs** to evaluate resource configurations against compliance requirements. Configuration history supports investigations; remediation actions can invoke automation.

Get practice exams and lessons for AWS Certified CloudOps Engineer - Associate