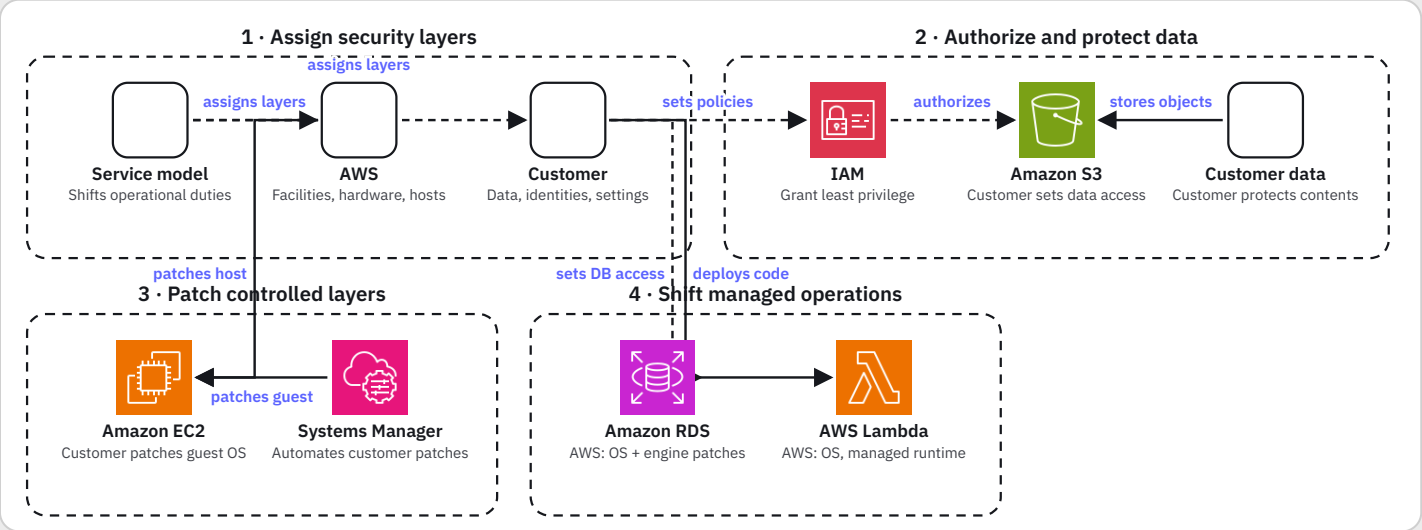
DOMAIN 2 · SECURITY AND COMPLIANCE · 30% OF THE EXAM · TASK STATEMENT 2.1

Understand the AWS shared responsibility model

Assign, authorize, patch, manage



1 Assign security layers

Security of the cloud belongs to AWS: facilities, hardware, physical networking and virtualization. Customers secure their workloads in the cloud; the service model sets the operational boundary.

2 Authorize and protect data

Least privilege limits IAM permissions. Customers classify data and configure S3 access, bucket policies, public access controls and encryption settings; AWS operates the storage infrastructure.

3 Patch controlled layers

Shared controls cover patch and configuration management: AWS manages its infrastructure; customers manage EC2 guest OS, applications and settings. Systems Manager automates customer work without transferring ownership.

4 Shift managed operations

More managed shifts operations to AWS: RDS OS/database-engine patching; Lambda OS/managed-runtime maintenance. Customers retain RDS data/access/settings and Lambda code/dependencies/settings.

Exam traps

- **Managed does not mean responsibility-free**: AWS operates RDS and Lambda infrastructure; customers still protect data, configure access and maintain their own code.
- **Host OS is not guest OS**: AWS patches the EC2 physical host; customers patch the instance's guest OS and applications, even when Systems Manager performs the automation.
- **AWS compliance is not customer compliance**: AWS certifications do not automatically make a workload compliant; customer permissions, data handling and configuration still matter.

Get practice exams and lessons for AWS Certified Cloud Practitioner

AWS Certified Cloud Practitioner Cheat Sheet

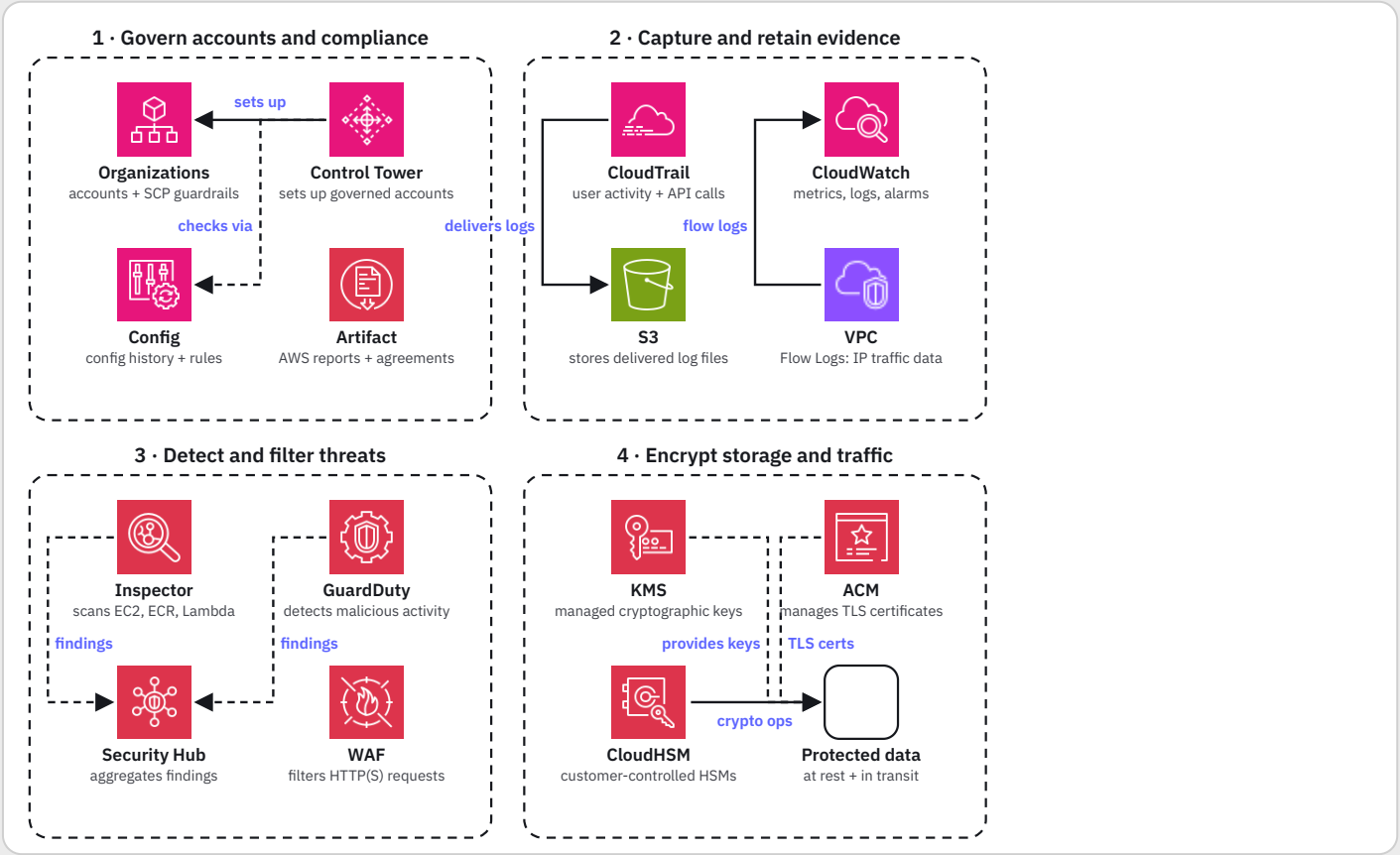
CLF-C02 · Domain 2 of 4

BlowStack

DOMAIN 2 · SECURITY AND COMPLIANCE · TASK STATEMENT 2.2

Understand AWS Cloud security, governance, and compliance concepts

Govern, record, detect, encrypt



1 Govern accounts and compliance

For **compliance evidence**, Artifact supplies AWS reports and agreements. Verify service, Region, and industry scope; AWS compliance does not certify customer workloads. Residency includes replicas, backups, and logs.

2 Capture and retain evidence

For **API activity**, CloudTrail records who did what. CloudWatch monitors metrics and logs; S3 retains delivered logs. VPC Flow Logs require configuration and capture traffic metadata, not packet payloads.

3 Detect and filter threats

For **security findings**, Inspector finds software vulnerabilities, GuardDuty detects threats, and Security Hub aggregates findings. WAF filters web requests; detection alone does not remediate resources.

4 Encrypt storage and traffic

For **key control**, KMS provides managed key services; CloudHSM provides dedicated HSMs under customer control. ACM manages TLS certificates, not stored-data encryption. Encryption still requires protected keys and permissions.

Exam traps

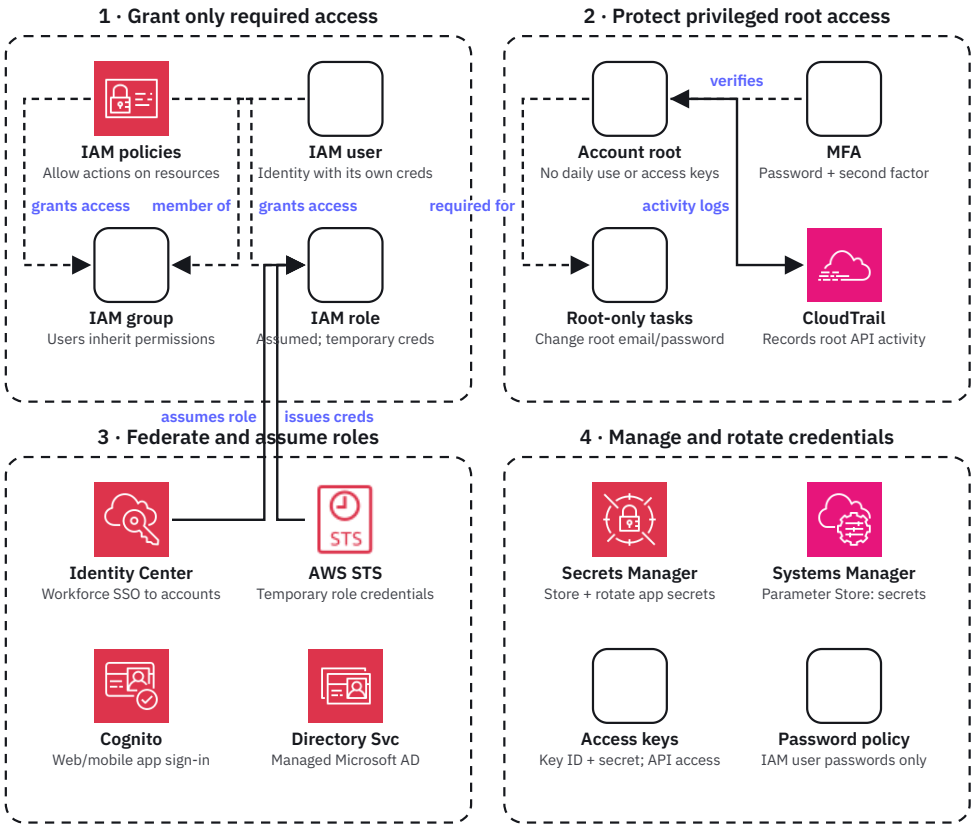
- **Shared responsibility**: AWS secures the cloud infrastructure; customers secure their data, access, and configurations. The boundary varies by service; AWS certification is not customer compliance.
- **Audit versus monitor**: CloudTrail records API activity; Config tracks resource configurations and rule compliance; CloudWatch monitors metrics and logs. SCPs limit permissions but never grant them.
- **Shield versus WAF**: AWS Shield provides DDoS protection; AWS WAF filters web requests using rules. Shield Standard is automatic; neither service replaces vulnerability scanning or threat detection.

Get practice exams and lessons for AWS Certified Cloud Practitioner

DOMAIN 2 · SECURITY AND COMPLIANCE · TASK STATEMENT 2.3

Identify AWS access management capabilities

Authorize, protect, federate, manage credentials



1 Grant only required access

Apply **least privilege** to actions and resources. Groups contain users, not roles. AWS-managed and customer-managed policies are reusable; custom inline policies belong to one identity. Explicit deny overrides allow.

2 Protect privileged root access

Reserve **root** for tasks requiring root credentials, not daily administration. Protect it with MFA, a strong unique password and secured recovery email. CloudTrail records activity; it does not prevent misuse.

3 Federate and assume roles

Use **federation** to reuse an external identity provider. Identity Center provides workforce SSO; Cognito serves application users; Directory Service integrates Microsoft AD. Cross-account roles require trust and permissions.

4 Manage and rotate credentials

Secrets Manager supports automatic rotation when configured. Systems Manager Parameter Store stores encrypted SecureString values without built-in rotation. Prefer role credentials to long-lived keys; never embed keys in code.

Exam traps

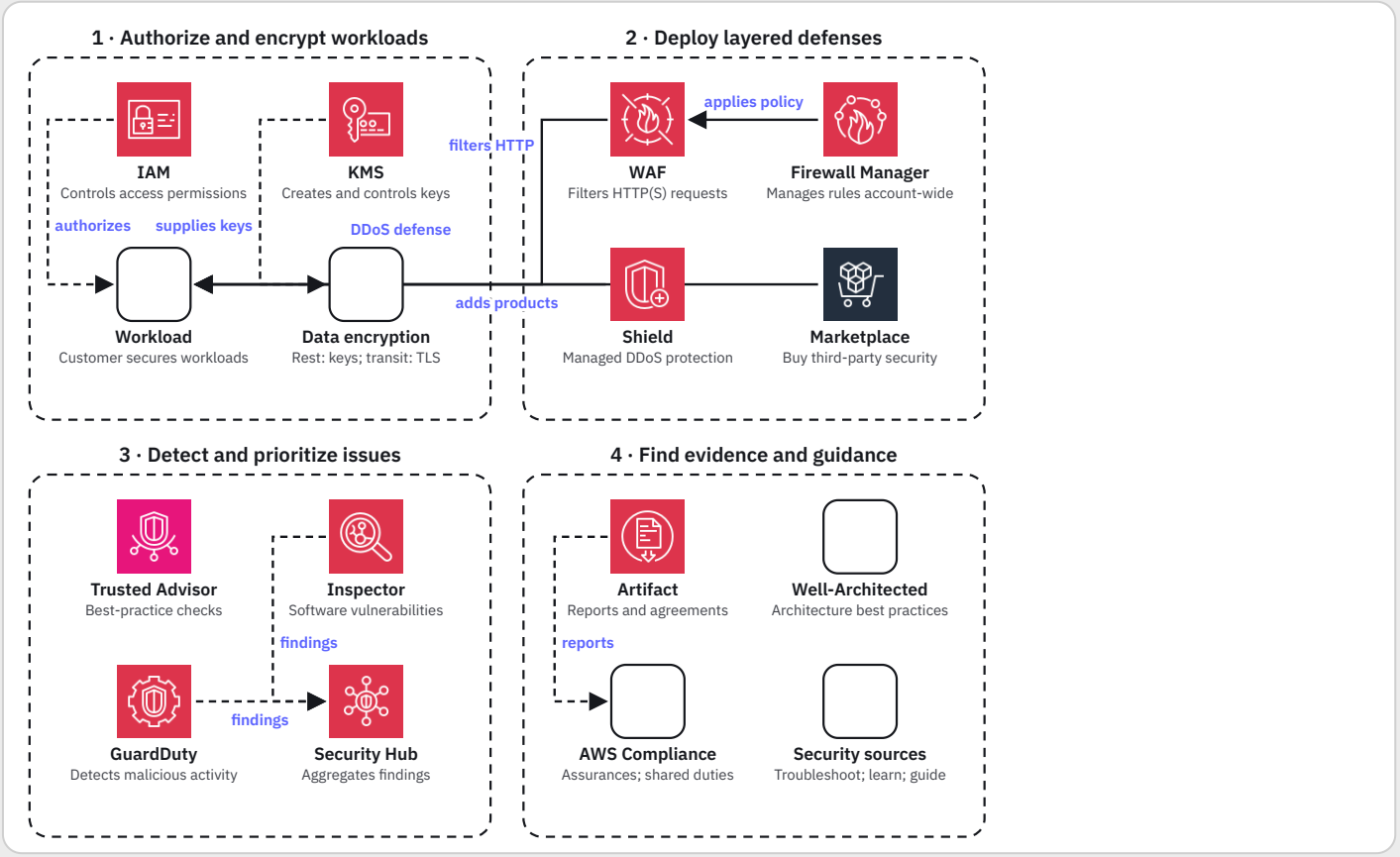
- **Authentication ≠ authorization**: MFA verifies identity; policies grant permissions. MFA does not automatically protect API calls made with long-lived access keys.
- **Password policies** govern IAM user passwords: length, reuse and expiration. They do not govern root passwords or access keys; federated passwords follow the identity provider's policy.
- **IAM access keys do not rotate automatically**: create a replacement, update consumers, then deactivate/delete the old key. Storing a credential does not automatically enable its rotation.

Get practice exams and lessons for AWS Certified Cloud Practitioner

DOMAIN 2 · SECURITY AND COMPLIANCE · TASK STATEMENT 2.4

Identify components and resources for security

Authorize, encrypt, defend, investigate, verify



1 Authorize and encrypt workloads

IAM controls **permissions**; KMS manages encryption keys; Amazon VPC provides network isolation. Encryption at rest protects stored data; encryption in transit protects network traffic.

2 Deploy layered defenses

WAF filters web exploits; Shield addresses DDoS. Firewall Manager applies policies **across accounts**. Marketplace offers third-party security products, not AWS compliance reports.

3 Detect and prioritize issues

The **signal** determines the service: GuardDuty detects threats; Inspector finds software vulnerabilities; AWS Config evaluates resource configurations; Amazon Macie discovers sensitive data in Amazon S3.

4 Find evidence and guidance

AWS Knowledge Center provides **troubleshooting**; AWS Security Center provides security resources; AWS Security Blog provides practical guidance. The AWS Well-Architected Framework guides architecture reviews.

Exam traps

- Security Hub **aggregates findings**; Inspector scans for vulnerabilities. Trusted Advisor recommends improvements across several categories, not just security; recommendations do not imply automatic fixes.
- Artifact supplies **compliance evidence**, not automatic customer compliance. AWS secures underlying infrastructure; customers remain responsible for their data, permissions, and workload configurations.
- Shield Standard provides **automatic DDoS protection** at no additional charge; Shield Advanced is paid. WAF filters web requests, while Firewall Manager centrally manages policies across accounts.

Get practice exams and lessons for AWS Certified Cloud Practitioner

DOMAIN 2 · SECURITY AND COMPLIANCE · WHAT TO REMEMBER

Concepts and services of Security and Compliance

Concepts to know

AWS shared responsibility model

AWS secures the cloud; customers secure what they put in it. **Responsibility shifts with the service**: customers patch guest operating systems on EC2, while AWS manages the operating systems for RDS and Lambda. Customers retain data and access responsibilities.

Least privilege

Grant only the actions and resource access required for a task. **Explicit deny overrides allow**; access is implicitly denied unless allowed. Administrative access is not the default choice for users or workloads.

AWS Compliance

AWS compliance certifications do not automatically make customer workloads compliant. **Verify service and geographic scope**, then implement customer controls and retain evidence for applicable industry, legal, and contractual requirements.

Core services



AWS Identity and Access Management (IAM)

Controls access through users, groups, roles, and policies. Choose **IAM roles** for workload or cross-account access using temporary credentials rather than long-term access keys.



AWS CloudTrail

Records account activity and API calls for auditing. Choose **who did what and when**; CloudWatch covers operational monitoring, while AWS Config tracks resource configurations and compliance.



AWS Artifact

Provides on-demand AWS compliance reports and agreements. Choose **AWS compliance evidence**, such as audit reports, rather than workload monitoring or customer configuration assessment.

Get practice exams and lessons for AWS Certified Cloud Practitioner