AWS Certified DevOps Engineer - Professional Cheat Sheet

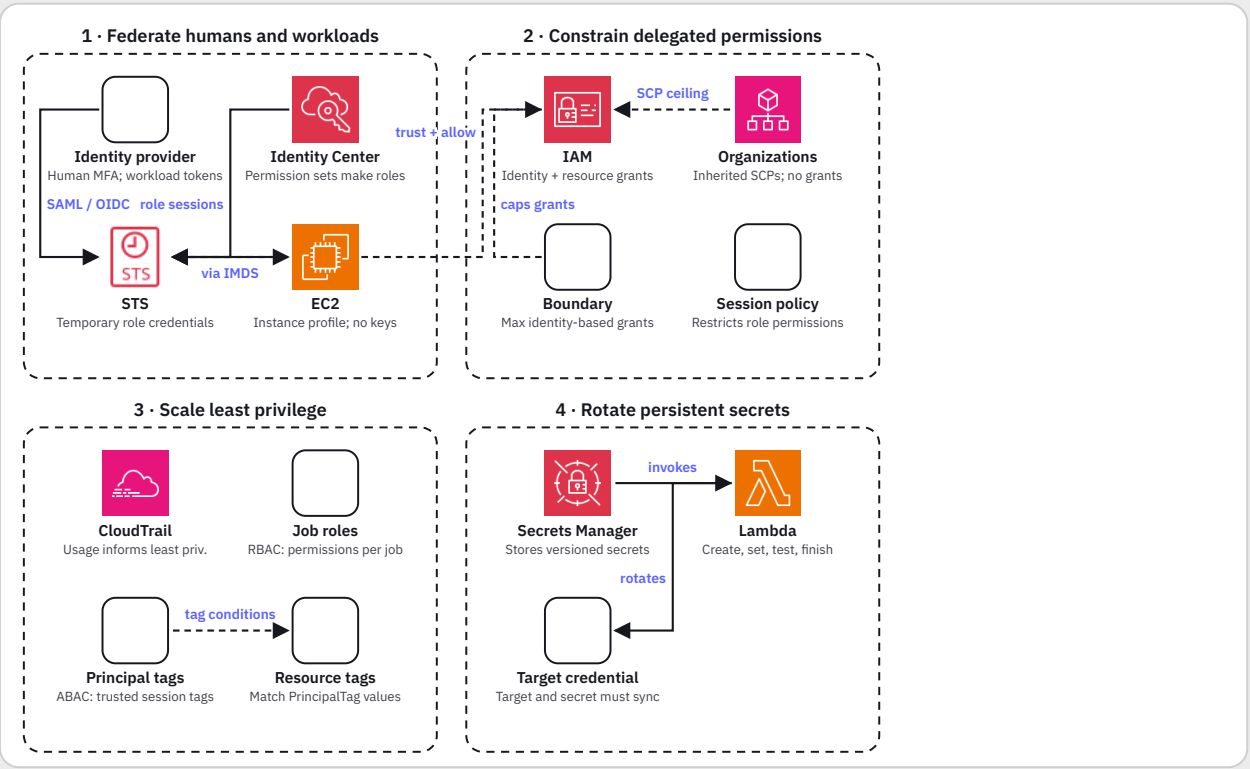
DOP-C02 · Domain 6 of 6

BlowStack

DOMAIN 6 · SECURITY AND COMPLIANCE · 17% OF THE EXAM · TASK STATEMENT 6.1

Implement techniques for identity and access management at scale

Federate, constrain, authorize, rotate



1 Federate humans and workloads

Choose **federation** over IAM users for workforce access. SAML uses AssumeRoleWithSAML; OIDC uses AssumeRoleWithWebIdentity. Identity Center assigns account roles; EC2 retrieves automatically renewed credentials through IMDS.

2 Constrain delegated permissions

Delegate role creation with a **permissions boundary**; require it and prevent removal. SCPs constrain member accounts, including root, not the management account. Allow-list SCPs need an allow at every hierarchy level.

3 Scale least privilege

Use **ABAC** for changing teams and resources; compare aws:PrincipalTag with supported resource-tag condition keys. Restrict tagging and sts:TagSession to prevent escalation. Use CloudTrail activity to refine least privilege.

4 Rotate persistent secrets

Choose **Secrets Manager** for persistent application secrets. Use managed rotation where supported; otherwise configure a Lambda rotation function. Rotation updates the target and stored secret; consumers must retrieve refreshed values.

Exam traps

- **Cross-account AssumeRole** requires caller permission and target-role trust; neither alone suffices. IAM groups organize users, cannot contain roles, and cannot be assumed.
- **Explicit deny wins**. Boundaries and SCPs grant nothing. A same-account resource-policy grant directly to a role-session ARN is not capped by implicit boundary or session-policy denies.
- **Secrets Manager rotation is not IAM access-key rotation**. IAM keys need separate automation; storing a key does not rotate it. Prefer automatically renewed role credentials for AWS workloads.

Get practice exams and lessons for AWS Certified DevOps Engineer - Professional

AWS Certified DevOps Engineer - Professional Cheat Sheet

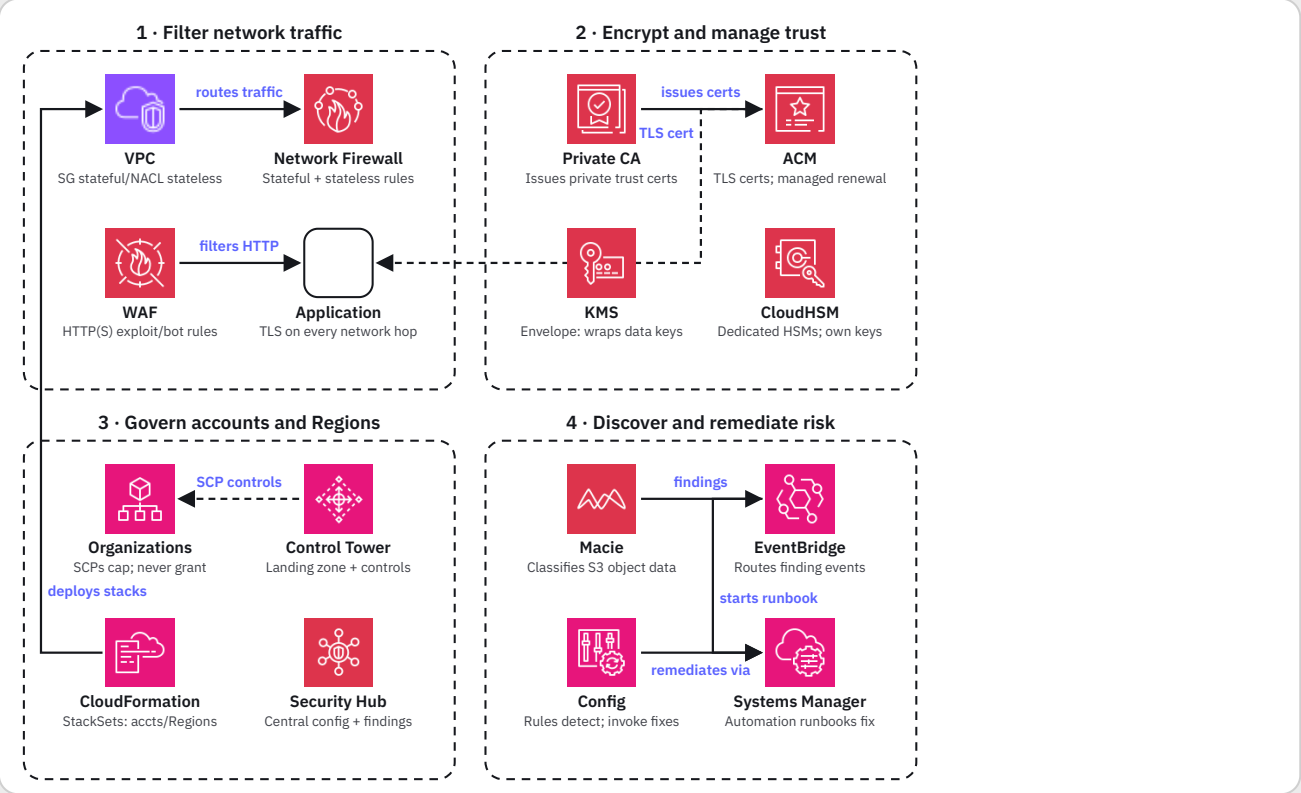
DOP-C02 · Domain 6 of 6

BlowStack

DOMAIN 6 · SECURITY AND COMPLIANCE · TASK STATEMENT 6.2

Apply automation for security controls and data protection

Filter, encrypt, govern, remediate



1 Filter network traffic

Use **routed inspection** for Network Firewall; keep forward/return paths symmetric. WAF filters HTTP(S); Shield mitigates DDoS. SGs allow only; NACLs allow/deny and need return-path rules.

2 Encrypt and manage trust

Choose **key custody**: KMS integrates with AWS; CloudHSM provides dedicated HSM control. ACM renews eligible managed certificates; private CA trust must be distributed. Envelope encryption wraps data keys, not bulk data.

3 Govern accounts and Regions

Use **StackSets** for repeatable account/Region deployments; use Security Hub central configuration for standards across OUs and linked Regions. Control Tower controls govern enrolled accounts; SCPs never grant access.

4 Discover and remediate risk

Use **Macie** for S3 sensitive-data discovery; enable discovery in each required Region. EventBridge can trigger remediation workflows. Config detects resource noncompliance; Systems Manager Automation performs fixes.

Exam traps

- S3 encryption is not authorization: **SSE-KMS** access requires S3 permission and KMS authorization; cross-account sharing needs a customer managed key, not the AWS managed aws/s3 key.
- A finding is not a fix: **Security Hub and Config** do not block attacks merely by reporting them; configure EventBridge actions or Config remediation and the required permissions.
- ACM does not renew everything: **imported certificates** require external renewal and reimport; exporting a managed certificate does not automatically deploy renewed copies to external endpoints.

Get practice exams and lessons for AWS Certified DevOps Engineer - Professional

AWS Certified DevOps Engineer - Professional Cheat Sheet

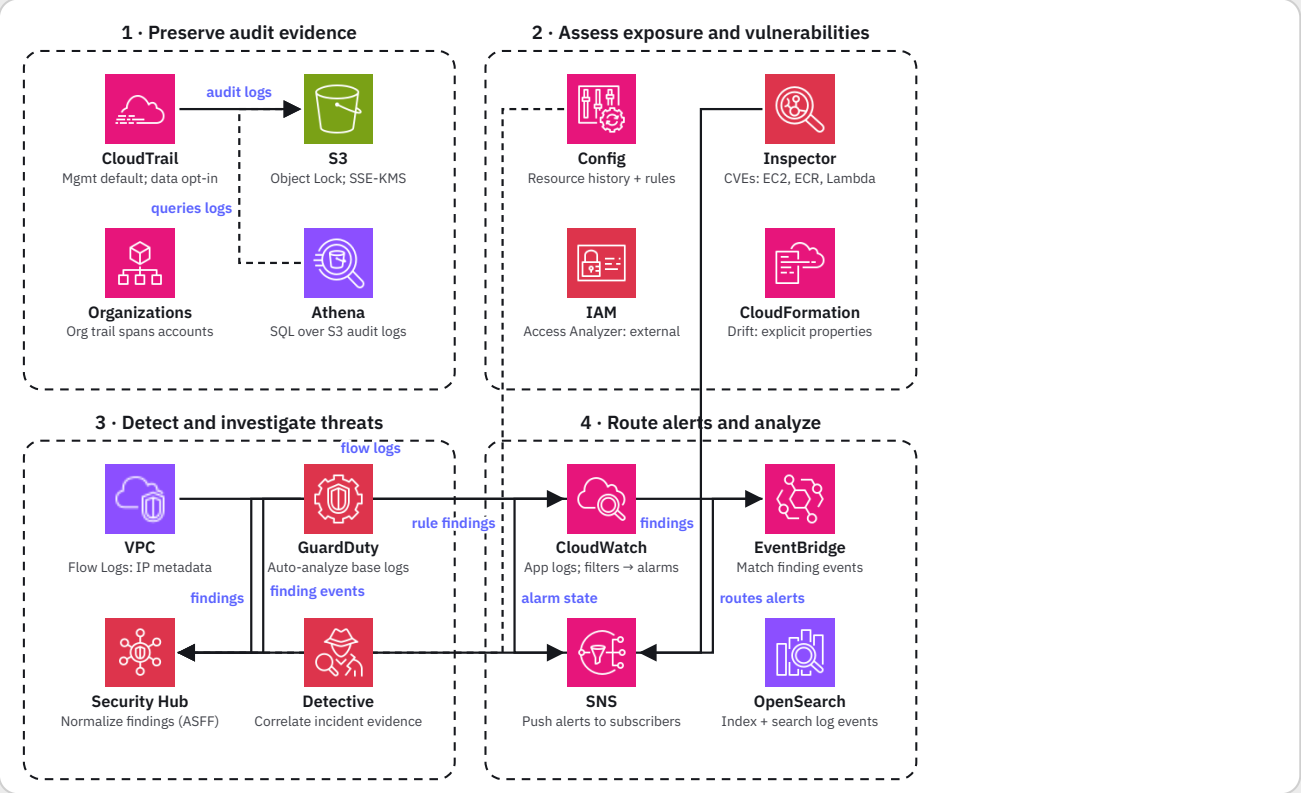
DOP-C02 · Domain 6 of 6

BlowStack

DOMAIN 6 · SECURITY AND COMPLIANCE · TASK STATEMENT 6.3

Implement security monitoring and auditing solutions

Record, assess, detect, alert



1 Preserve audit evidence

Organization trail covers member accounts; use a multi-Region trail, enable data events explicitly, validate log files, and preserve S3 evidence with Object Lock and retention.

2 Assess exposure and vulnerabilities

Config rules assess configuration compliance; Inspector finds software CVEs; IAM Access Analyzer finds external access. CloudFormation drift checks supported, explicitly set properties—not general compliance.

3 Detect and investigate threats

GuardDuty analyzes independent telemetry; enabling VPC Flow Logs is not required. Security Hub aggregates findings; Detective correlates identities, API activity and network behavior to reconstruct incidents.

4 Route alerts and analyze

Metric threshold/anomaly → CloudWatch alarm → SNS; finding event → EventBridge → SNS. Set log retention and data protection masking; tune thresholds and suppression to reduce false positives.

Exam traps

- **Log validation detects tampering**; it does not prevent deletion. S3 Object Lock protects retained versions; SSE-KMS protects confidentiality, not public-access configuration.
- **Flow Logs contain metadata**, not packet payloads. An S3 policy denying aws:SecureTransport=false enforces HTTPS; encryption at rest does not secure network traffic.
- **Access Analyzer is not leaked-key detection**; GuardDuty detects suspicious credential use. Exposed keys require immediate deactivation and replacement, not merely an alert.

Get practice exams and lessons for AWS Certified DevOps Engineer - Professional

AWS Certified DevOps Engineer - Professional Cheat Sheet

DOP-C02 · Domain 6 of 6

BlowStack

DOMAIN 6 · SECURITY AND COMPLIANCE · WHAT TO REMEMBER

Concepts and services of Security and Compliance

Concepts to know

Effective Permissions

Usable access depends on grants, policy limits, and request context. **Explicit deny overrides allow**; permissions boundaries and SCPs limit permissions but never grant them. Cross-account role access requires caller permission and role trust.

Defense in Depth

Layered preventive, detective, and response controls reduce reliance on one safeguard. **Match the control to the threat**: network filtering, application filtering, encryption, and configuration evaluation address different risks.

Audit Logging

Audit records establish who acted, when, and against which resource. **Choose complementary evidence sources**: API activity, configuration history, and network flows answer different questions; centralized, protected retention supports investigations.

Core services



AWS Identity and Access Management (IAM)

Use **roles and temporary credentials** for workload and federated access. Permissions boundaries cap delegated permissions; tag-based conditions scale access when tag changes are controlled.



AWS CloudTrail

Choose **API activity auditing** to identify actors and actions. Organization trails centralize account coverage; data events require configuration, and log validation detects tampering.



AWS Config

Choose **configuration history and compliance evaluation**, not API attribution or threat detection. Rules detect noncompliance; remediation can invoke automated corrective actions.

Get practice exams and lessons for AWS Certified DevOps Engineer - Professional