AWS Certified DevOps Engineer - Professional Cheat Sheet

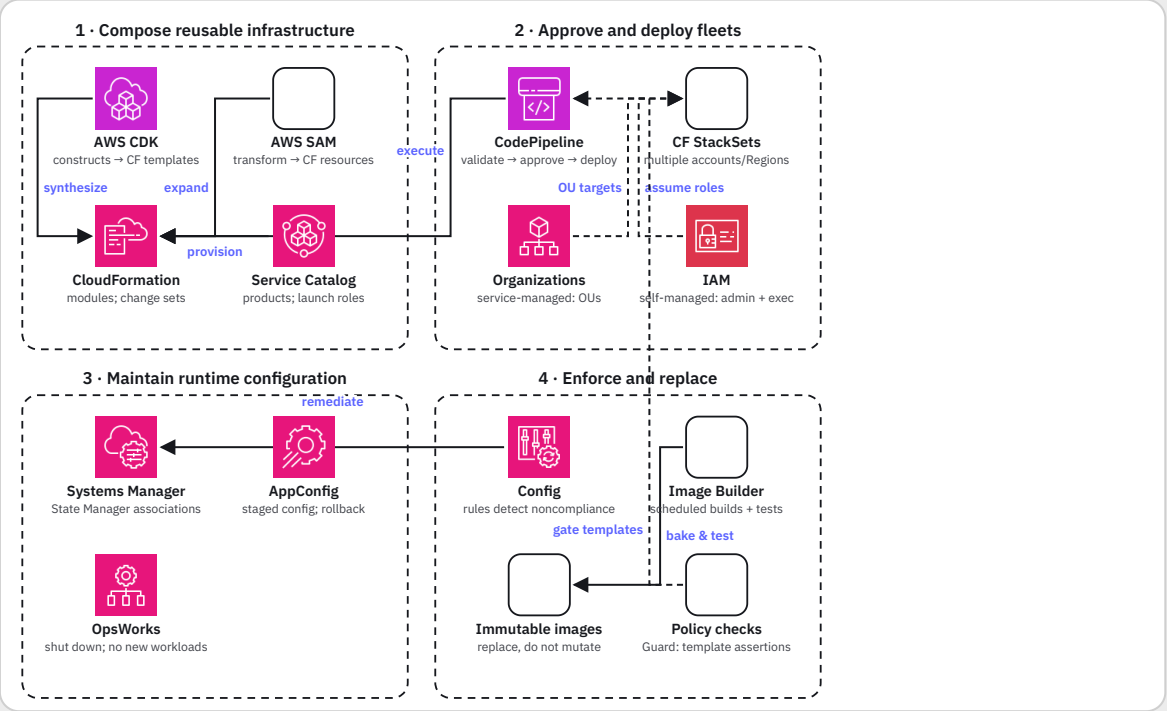
DOP-C02 · Domain 2 of 6

BlowStack

DOMAIN 2 · CONFIGURATION MANAGEMENT AND IAC · 17% OF THE EXAM · TASK STATEMENT 2.1

Define cloud infrastructure and reusable components to provision and manage systems throughout their lifecycle

Compose, approve, configure, enforce



1 Compose reusable infrastructure

Reusable IaC: CDK constructs generate templates; SAM specializes in serverless resources; CloudFormation modules package resource patterns. Declarative desired state supports repeatable updates; retries still require idempotency.

2 Approve and deploy fleets

Version-controlled IaC → CI/CD validation → independent approval → execution preserves **separation of duties**. StackSets use service-managed Organizations integration or self-managed IAM roles; execution permissions stay least privilege.

3 Maintain runtime configuration

Use **State Manager** for recurring OS desired state; Automation executes runbooks. AppConfig deploys application settings with validation and alarm-triggered rollback. OpsWorks support ended May 1, 2024.

4 Enforce and replace

Immutable infrastructure replaces hosts from tested AMIs or container images. Config evaluates running resources; policy checks gate templates before deployment. Image builds alone do not replace running hosts.

Exam traps

- **Change sets preview**, not deploy; execution is separate. Service Catalog constrains approved products and launch permissions; it does not replace template validation.
- **OU auto-deployment is optional**: service-managed StackSets require Organizations trusted access. Self-managed StackSets require administration and execution roles with cross-account trust.
- **Detection is not repair**: Config rules assess compliance; CloudFormation drift checks supported properties. Neither automatically repairs drift; Config-to-Systems Manager remediation needs configuration.

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

AWS Certified DevOps Engineer - Professional Cheat Sheet

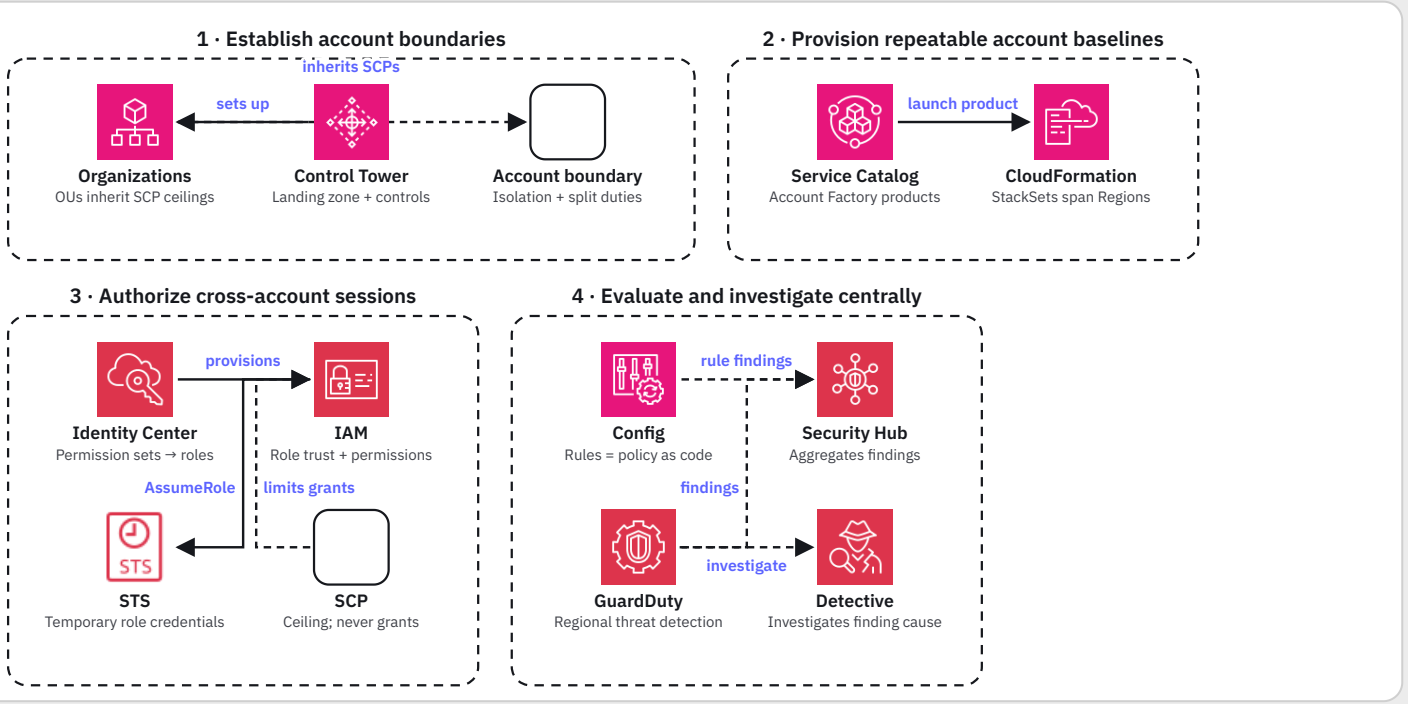
DOP-C02 · Domain 2 of 6

BlowStack

DOMAIN 2 · CONFIGURATION MANAGEMENT AND IAC · TASK STATEMENT 2.2

Deploy automation to create, onboard, and secure AWS accounts in a multi-account or multi-Region environment

Isolate, provision, authorize, govern



1 Establish account boundaries

AWS Control Tower automates a governed landing zone and Account Factory. Organizations alone supplies account hierarchy and policies. Separate workload, security and log-archive accounts reduce blast radius.

2 Provision repeatable account baselines

Service-managed StackSets use Organizations trusted access to target OUs. Enable automatic deployment for new accounts; select target Regions explicitly. Versioned IaC standardizes baselines; idempotent retries avoid duplicates.

3 Authorize cross-account sessions

AssumeRole across accounts needs caller permission and target-role trust. Effective permissions respect SCPs, boundaries and session policies; explicit deny wins. Identity Center permission sets provision account roles.

4 Evaluate and investigate centrally

Delegated administrators centralize security management per service. Configure organization enrollment and required Regions; aggregation alone neither enables regional detection nor automatically remediates findings.

Exam traps

- An SCP **grants no permissions**; an action needs allowance at every root→OU→account level. SCPs do not restrict the management account or service-linked roles.
- A **detective control** reports noncompliance; it does not block deployment. Control Tower preventive controls use SCPs; proactive controls use CloudFormation hooks.
- **StackSets do not create accounts**; Account Factory provisions accounts. StackSets deploy resource baselines into existing accounts, including newly added OU accounts when automatic deployment is enabled.

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

AWS Certified DevOps Engineer - Professional Cheat Sheet

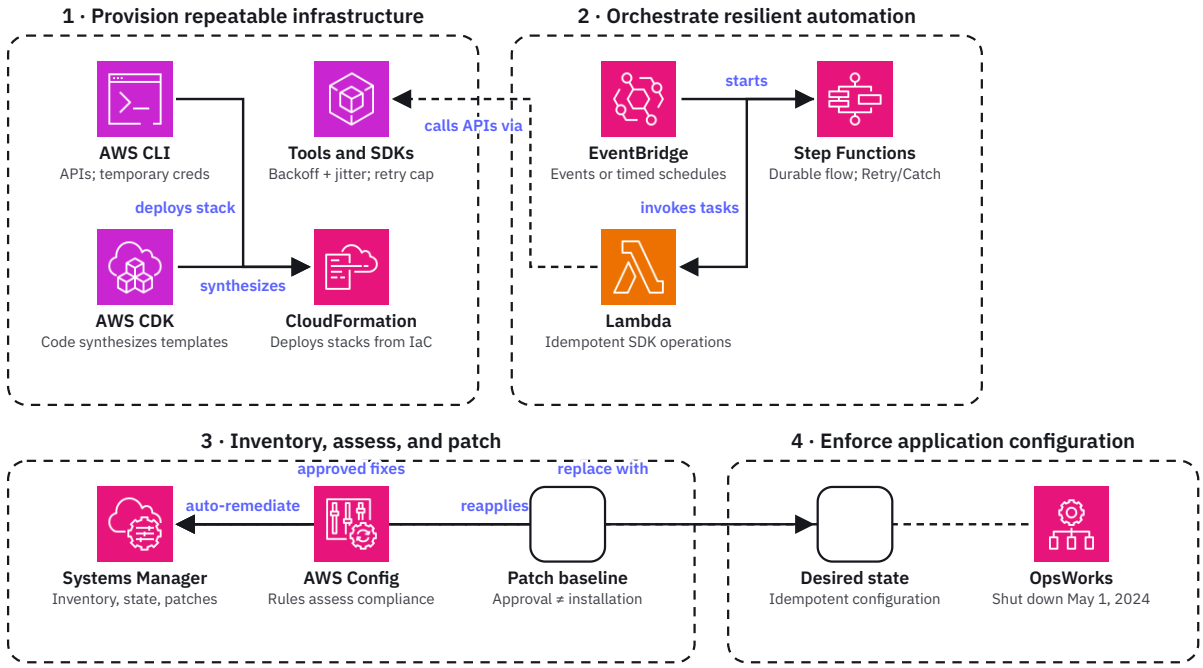
DOP-C02 · Domain 2 of 6

BlowStack

DOMAIN 2 · CONFIGURATION MANAGEMENT AND IAC · TASK STATEMENT 2.3

Design and build automated solutions for complex tasks and large-scale environments

Provision, orchestrate, patch, enforce



1 Provision repeatable infrastructure

Choose **IaC** for repeatable, reviewed infrastructure: CDK synthesizes CloudFormation templates; CloudFormation deploys them. CLI/SDK call APIs with temporary credentials; ad hoc API calls are not declarative IaC.

2 Orchestrate resilient automation

Choose **Step Functions** for durable multi-step coordination, Retry/Catch and bounded backoff; Lambda runs code tasks. EventBridge routes events or schedules starts; retries require idempotent side effects.

3 Inventory, assess, and patch

Choose **Patch Manager** to install approved patches; baselines only approve, Maintenance Windows schedule execution. Systems Manager Inventory collects metadata; AWS Config evaluates resource compliance, not OS patching.

4 Enforce application configuration

Choose **State Manager** associations for recurring OS/application configuration management; reapply desired state on schedule to correct drift. AWS OpsWorks is shut down and is not an option for new workloads.

Exam traps

- **Config ≠ stack drift**: Config evaluates resource rules; CloudFormation drift compares supported actual properties with templates. Config repair requires configured Automation remediation.
- **Retries ≠ exactly once**: Lambda and workflow retries can repeat side effects. Use idempotency keys or conditional updates; exponential backoff with jitter handles throttling, not duplicates.
- **Patch compliance ≠ full compliance**: Patch Manager reports patch state; Inventory gathers metadata. Neither proves all application settings or AWS Config rules are compliant.

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

AWS Certified DevOps Engineer - Professional Cheat Sheet

DOP-C02 · Domain 2 of 6

BlowStack

DOMAIN 2 · CONFIGURATION MANAGEMENT AND IAC · WHAT TO REMEMBER

Concepts and services of Configuration Management and IaC

Concepts to know

Infrastructure as code (IaC)

Infrastructure definitions make provisioning repeatable and reviewable. Choose **version-controlled, reusable templates** for standardized environments, with automated validation and approval gates before production deployment.

Configuration Drift

Drift is divergence from intended configuration. Distinguish **detection from remediation**: resource compliance checks identify violations, desired-state automation corrects settings, and immutable deployments replace instances.

Effective Permissions

Usable access depends on applicable grants, permission ceilings, and explicit denies. **SCPs restrict but never grant permissions**; cross-account role assumption requires caller authorization and a role trust policy.

Core services



AWS CloudFormation

Use **StackSets for multi-account, multi-Region provisioning**, change sets to preview updates, and drift detection to identify supported resource differences; detection does not remediate drift.



AWS Systems Manager

Choose **State Manager for recurring desired-state enforcement**, Patch Manager for patching, Automation for operational runbooks, and Run Command for immediate commands on managed nodes.



AWS Organizations

Use **OUs and SCPs for centralized account governance**. SCPs set permission ceilings for member accounts; choose AWS Control Tower for a governed landing zone and automated account provisioning.

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