

Understanding Systems Operations on AWS

SYSTEMS OPERATIONS · CORE SERVICES · RESOURCE SCOPE · SERVICE LIMITS · IAM · AWS CLI

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

- 01 Automate for repeatability:** Systems operations is the work to build (create), test, deploy, monitor, maintain, and safeguard complex computing systems. Packaging infrastructure as a **script, program, or template** — a shell script, a Python/Ruby/C# app, or **AWS CloudFormation** — makes deployment **repeatable on demand**: define it once, then recreate it in other Regions or as dev and test environments that match production.
- 02 Three core service areas:** **Network** → **Amazon VPC** (a logically isolated virtual network where you set IP ranges, routing, gateways, and security), **Compute** → **Amazon EC2** (virtual servers launched from **AMIs**; scalable and optimizable), and **Access** → **IAM** (who can do what).
- 03 Know the resource scope:** Every feature is **global**, **Regional**, or bound to an **Availability Zone**. IAM, Route 53 hosted zones, and CloudFront are global; S3 buckets, AMIs, EBS snapshots, ElastiCache clusters, CloudWatch metrics, and VPCs are Regional; EC2 instances, EBS volumes, subnets, and RDS instances live in one AZ — and an EBS volume attaches only to an instance **in the same AZ**.
- 04 IAM = authentication + authorization:** IAM (a free account feature) controls **who** may access resources (authentication) and **what** actions they may take, down to individual API calls (authorization). Use **least privilege**, prefer **roles** over shared keys, and remember: an explicit **Deny always overrides any Allow**, regardless of evaluation order.
- 05 CLI — filter, query, dry-run:** The AWS CLI automates AWS through `aws <service> <operation> --parameters. --filter` restricts results **server-side**; `--query` (JMESPath) limits displayed fields **client-side**; `--dry-run` checks permissions **without making the request**. Default output is JSON (also table and text).

02 KEY TERMS

TERM	DEFINITION
Systems operations	The responsibilities and tasks to build (create), test, deploy, monitor, maintain, and safeguard complex computing systems
Amazon VPC	Amazon Virtual Private Cloud — a logically isolated virtual network, defined within a Region, into which you launch resources such as EC2 instances
Amazon EC2	Amazon Elastic Compute Cloud — provisions scalable, optimizable virtual servers (instances) in the cloud
AMI	Amazon Machine Image — a reusable image of a server used to launch instances; it is Regional, so copy it to launch in another Region
IAM	AWS Identity and Access Management — centrally manages authentication and authorization to AWS resources; a feature of an account at no charge
IAM role	An identity with a permissions policy that is assumed to obtain temporary security credentials; usable by users, applications, or services such as EC2
Identity federation	Single sign-on using corporate-directory credentials via open standards such as SAML 2.0, exchanged between an identity provider (IdP) and AWS
Access keys	An access key ID and secret access key that authenticate programmatic access to the API, AWS CLI, and SDKs
MFA	Multi-factor authentication — an extra layer of security that can be enabled for the root account and for IAM users
Service limit	A default account quota; soft limits can be raised with a Support case, hard limits (e.g., SNS 100 Subscribe/sec) cannot be changed

TERM	DEFINITION
Root user	The identity tied to the account's sign-up email and password; best practice is to use it only to create the first IAM user, then lock it away
aws configure	The AWS CLI command that sets defaults: access key ID, secret access key, default Region, and output format

03 RESOURCE SCOPE ON AWS

know what is global, Regional, or AZ-bound

SCOPE	EXAMPLE RESOURCES	RULE OF THUMB
Global	IAM users, groups, roles · Route 53 hosted zones · CloudFront distributions	Referenced across all Regions
Regional	S3 buckets · AMLs · CloudWatch metrics · EBS snapshots · ElastiCache clusters · VPCs	Pick a Region; copy AMLs to reuse elsewhere
Availability Zone	EC2 instances · EBS volumes · subnets · RDS DB instances	EBS attaches only within the same AZ

04 IAM AUTHENTICATION: TWO ACCESS TYPES

an IAM user can have one or both

PROGRAMMATIC ACCESS <i>for the API, AWS CLI, and SDKs</i> — Authenticates with an access key ID and secret access key — Grants access to the AWS APIs, AWS CLI, and SDKs — The path used to automate and script AWS	AWS MANAGEMENT CONSOLE ACCESS <i>for the web interface</i> — Uses the account ID or alias, IAM user name, and password — If MFA is enabled, prompts for a code — A simple web interface to most AWS services
---	---

05 AWS CLI COMMAND ANATOMY

01 aws — the base command → **02** service — e.g. ec2, s3 → **03** operation — e.g. run-instances, describe-instances → **04** parameters — prefixed with -- (e.g. --instance-id i-1234...) → **05** options — e.g. --output json

06 AWS CLI OPTIONS AND OUTPUT

filter server-side · query client-side

OPTION / SETTING	WHAT IT DOES
--filter	Restricts the result set on the server side (e.g. only Windows instances)
--query	Limits which fields are displayed , on the client side, using JMESPath (e.g. Reservations[0].Instances[0].State.Name)
--dry-run	Checks for required permissions without making the request — DryRunOperation if allowed, UnauthorizedOperation if not
--output	Sets response format: json (default), table , or text
aws help	Shows syntax and examples for any command (e.g. aws ec2 help)

- × “IAM is Regional, so I create users per Region.” — IAM users, groups, and roles are **global** and are referenced across every Region in the account (as are Route 53 hosted zones and CloudFront distributions).
- × “I can attach this EBS volume to my instance in another AZ.” — No. An EBS volume attaches only to an EC2 instance in the **same Availability Zone**; create the volume in that AZ first.
- × “An AMI I create is available in every Region.” — AMIs are **Regional**. To launch from one in another Region, you must **copy the AMI** to that Region first.
- × “The 20-instance limit is fixed.” — That per-Region On-Demand cap is a **soft limit**; request a Service Limit Increase in the Support Center. **Hard limits** (e.g. SNS 100 Subscribe transactions/second) cannot be changed.
- × “--query filters on the server to cut data transferred.” — --query runs **client-side** (JMESPath) and only limits what is displayed; --filter is the **server-side** option that restricts the result set.
- × “If an Allow and a Deny both match, the last one evaluated wins.” — Evaluation **order has no effect**; an explicit **Deny always overrides any Allow**.
- × “Use the root user for day-to-day administration.” — Create an IAM user for admin work and **lock the root credentials away**; use root only for the few tasks that require it, and enable MFA on it.
- × “Access keys let me sign in to the console.” — Access keys are for **programmatic** access (API, CLI, SDKs). Console sign-in uses the IAM **user name and password** (plus MFA if enabled).

08 SELF-QUIZ

answers are upside-down below

- Q1** Which AWS service provides the logically isolated virtual network into which you launch resources such as EC2 instances?
- Q2** Name three AWS resource types whose scope is global rather than Regional.
- Q3** You want to attach a newly created EBS volume to a running EC2 instance. What must be true about the volume's location?
- Q4** On a new account you need to run more On-Demand instances of a type than the per-Region default allows. What is your recourse?
- Q5** IAM decides two things for every request. What are they?
- Q6** When both an explicit Deny and an Allow apply to the same request, what is the outcome, and does evaluation order matter?
- Q7** Which type of IAM credential authenticates programmatic access through the API, CLI, and SDKs?
- Q8** Which AWS CLI option verifies that you have the required permissions for an action without actually performing it?
- Q9** Which AWS CLI option restricts the returned result set on the server side?
- Q10** Which command configures AWS CLI defaults such as credentials, default Region, and output format?

ANSWER KEY (rotate the page)

Q1 Amazon VPC (Amazon Virtual Private Cloud) **Q2** IAM users/groups/roles, Amazon Route 53 hosted zones, and Amazon CloudFront distributions **Q3** It must be created in the same Availability Zone as the instance **Q4** It is a soft limit — open a case in the AWS Support Center and request a Service Limit Increase (often approved) **Q5** Authentication (who the principal is) and authorization (what actions on which resources they may perform) **Q6** The explicit Deny wins; evaluation order has no effect on the outcome **Q7** Access keys (an access key ID and a secret access key) **Q8** The --dry-run option **Q9** The --filter option **Q10** aws configure